****

P1 Determine the difference between normal activity and an incident

26 de junio de 2024

adrián gonzález iglesias

Máster sistemas multicloud

INSTITUTO TAJAMAR

**Índice**

Contenido

[**Índice** 1](#_Toc170200461)

[**Determine the difference between normal activity and an incident** 2](#_Toc170200462)

[**Activity overview** 2](#_Toc170200463)

[**Scenario** 3](#_Toc170200464)

[**Task 1. Grant permissions to an external account** 4](#_Toc170200465)

[**Task 2. Access the Event Threat Detection findings** 5](#_Toc170200466)

[**Task 3. Analyze the findings** 6](#_Toc170200467)

[**Task 4. Access the findings in Cloud Logging** 8](#_Toc170200468)

[**Task 5. Fix the finding** 9](#_Toc170200469)

[**Conclusion** 10](#_Toc170200470)

[**End your lab** 10](#_Toc170200471)

**Determine the difference between normal activity and an incident**

[Determina la diferencia entre la actividad normal y un incidente | Google Cloud Skills Boost](https://www.cloudskillsboost.google/paths/419/course_templates/969/labs/485942)

important icon **IMPORTANT:**  
  
desktop/labtop icon Make sure to complete this hands-on lab on a desktop/laptop only.  
  
check icon There are only 5 attempts permitted per lab.  
  
quiz target icon As a reminder – it is common to not get every question correct on your first try, and even to need to redo a task; this is part of the learning process.  
  
timer icon Once a lab is started, the timer cannot be paused. After 1 hour and 30 minutes, the lab will end and you’ll need to start again.  
  
tip icon For more information review the **Lab technical tips** reading.

**Activity overview**

Event Threat Detection is one of Security Command Center's (SCC) services. Event Threat Detection is a log-based threat analysis that continuously monitors Google Cloud logs for potential threats. When Event Threat Detection identifies suspicious activity, it generates a finding that you can investigate.

In this lab, you’ll analyze findings in the Google Cloud Security Command Center and examine related events in Cloud Logging.

**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.

**Task 1. Grant permissions to an external account**

In this task, you’ll grant project owner rights to an external gmail account. Granting owner rights to an external account will trigger the Event Threat Detection IAM detectors. Granting project owner rights to an external account is considered anomalous behavior or potentially malicious activity. Event Threat Detection will identify this activity as a threat and generate findings which you'll examine in the upcoming tasks.

1. In the Google Cloud console, in the **Navigation menu** (Navigation Menu icon), click **IAM & Admin** > **IAM**. The **IAM** page opens.

**Accedemos al apartado IAM dentro de la consola de Google Cloud en la sección de IAM & Admin:**

Interfaz de usuario gráfica

Descripción generada automáticamente

On the **View By Principals** tab, note the two student users that have been automatically configured for the qwiklabs.net organization. These two users are also the same users listed in the **Lab details** panel as **Google Cloud username 1** and **Google Cloud username 2**.

These two users have automatically been granted owner roles to the lab project by a service account as part of a normal provisioning process. This will trigger an alert finding or incident because an external principal has an owner role. However, because both users belong to the qwiklabs.net organization this alert is considered normal activity. You will examine this alert finding later.

**Como podemos ver a continuación, tenemos los dos usuarios correspondientes al laboratorio, la única diferencia entre uno y otro son los permisos, uno es propietario y otro tiene más permisos a parte de propietario, como son para manejar todos los recursos del proyecto, para poder ver todos los roles, etc.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. On the **View By Principals** tab, click **Grant Access**. The **Grant access** dialog displays.

**Dentro del apartado IAM, accedemos a GRANT ACCESS para configurar los permisos.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Under the **Add principals** section, in the **New principals** field, type **[bad.actor.demo@gmail.com](mailto:bad.actor.demo@gmail.com)**.

**En el apartado New principals, añadimos el tipo que nos indica el enunciado.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. Expand the **Select a role** drop-down menu, select **Basic**, and then select **Owner**.

**Un poco más abajo en Select a Role, seleccionamos Rol tipo Basic y de nivel de rol Owner, para otorgar permisos de Propietario.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Click **Save**.

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

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 qwiklabs.net organization.

**Comprobación en la sección IAM & Admin:**Interfaz de usuario gráfica

Descripción generada automáticamente

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

|  |
| --- |
| Grant permissions to an external account  Check my progress |

Escala de tiempo

Descripción generada automáticamente con confianza media

**Con esto conseguimos añadir una cuenta externa que tendrá como función activar una detección de amenazas de eventos dentro del apartado IAM.**

**De esta manera, comprobaremos y solucionaremos las amenazas producidas al añadir esta cuenta externa.**

**Ahora, comprobaremos que se han configurado estas funciones.**

**Task 2. Access the Event Threat Detection findings**

In this task, you’ll access the Event Threat Detection findings in the Security Command Center.

1. In the Google Cloud console, in the **Navigation menu** (Navigation Menu icon), click **Security > Findings**. The **Findings** page opens.

**Accedemos al apartado Findings dentro de Security en la consola de Google Cloud.**

Imagen que contiene Gráfico

Descripción generada automáticamente

You should notice three findings with high severities listed in the **Finding query results** panel. In this lab, you’ll examine two **Persistence: IAM anomalous grant** findings to determine whether the finding is normal activity or whether it is malicious.

***Note:****If the****Persistence: IAM anomalous grant****findings are not listed, you may have to wait a few minutes and refresh. Wait until both these active findings display before continuing.*

The **Persistence: IAM anomalous grant** indicates that an anomalous IAM grant was detected. This means that a user or service account was granted access to a resource that they should not have had access to. This could be a potential indication of a malicious actor attempting to gain unauthorized access to your environment.

**Next**, filter the findings to display a list of **Persistence: IAM anomalous grant** category findings.

**Ahora vamos a analizar hallazgos de seguridad en el entorno de IAM, enfocándonos en la categoría Persistencia: concesión anómala de IAM**. **Estos hallazgos indican que un usuario o cuenta de servicio ha recibido permisos inusuales para acceder a un recurso, lo cual podría ser una señal de un intento de acceso no autorizado.**

**Nuestro objetivo es determinar si estos hallazgos representan actividades normales o maliciosas. Primero, identificaremos y filtraremos estos hallazgos en el panel de resultados. Luego, evaluaremos cada hallazgo en detalle para entender el contexto de la concesión de permisos.**

1. In the **Quick filters** panel, in the **Category** section, select the checkbox for the **Persistence: IAM anomalous grant** category.

**En la sección Quick filters, seleccionamos la opción Persistence:IAM anomalous grant:**

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

***Note:****Selecting attributes with quick filters automatically adds them to the query. Notice that the Query preview is updated with the****Persistence: IAM anomalous grant****category you selected. You can locate specific findings or groups of findings by editing the findings query.*

The filter returns two **Persistence: IAM anomalous grant** findings.

**En el apartado Query editor, podíamos realizar otra consulta, dependiendo de nuestras necesidades.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Click the **Event time** column header to sort the findings in descending order, so that the earliest finding is at the top.

**De esta manera ordenamos los eventos del más antiguo primero, al más nuevo el último. Diferentes maneras de organizar los eventos para nuestra comodidad o necesidad.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Task 3. Analyze the findings**

In this task, you'll examine these findings to determine which is normal activity and which is a genuine incident.

1. In the **Findings query results** panel, in the **Category** column, click the **Persistence: IAM Anomalous Grant** finding with the earliest event time. The **Persistence: IAM Anomalous Grant** dialog opens on the **Summary** tab, which displays the finding summary.

**Entramos en la categoría para inspeccionarla un poco más a fondo, y podemos ver varias cosas.**

**El nivel de anomalia, el horario de cuando se ha producido, el nombre del servicio, el tipo de categoría, etc.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Tabla

Descripción generada automáticamente con confianza baja

1. Find the **Principal email** row. This is the user account that granted the owner role to the user. Notice that the service account belongs to the qwiklabs.net organization. With this information, you can establish that this finding represents normal and expected activity.

**Lo hemos mostrado antes, pero podemos ver que la cuenta de Gmail que otorgó el rol de propietario de la anomalía al usuario es la del student04.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click the **Source Properties** tab, and expand **properties > sensitiveRoleGrant > members**. Again, the email address listed for **principalEmail** is the user that granted the owner role, and the email address(es) listed for **members** is the user that was granted the owner role.

**A continuación, observamos que el usuario nombrado antes (student04) es el que ha asignado la cuenta externa para controlar las amenazas nombradas al principio del proyecto.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Which user was granted the owner role in the earliest Persistence: IAM Anomalous Grant finding record?

* A Compute Engine service account
* None of these options
* The external user bad.actor.demo@gmail.com
* A user belonging to the qwiklabs.net organization

**Next**, you'll locate the malicious activity associated with the external user account you had granted access to: bad.actor.demo@gmail.com.

1. Click the close (**X**) button to return to the **Findings** page.
2. In the **Findings query results** panel, in the **Category** column, click on the **Persistence: IAM Anomalous Grant** findings record with the latest event time.

**Observamos la hora actualizada del evento en el apartado event time.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Note the value on the **Principal email** row. This is the user account email address that granted the owner role to the user.

**Anotamos de nuevo el Gmail principal del evento.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Click **Source Properties** tab, and expand **properties > sensitiveRoleGrant > members**. You should notice the user account **[bad.actor.demo@gmail.com](mailto:bad.actor.demo@gmail.com" \t "_blank)**, which is an external user account. With this information, you can establish that this finding is associated with an unauthorized and malicious actor.

**Anotamos la cuenta externa, añadida en el primer apartado del proyecto.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Con todas estas comprobaciones responderemos a las preguntas marcando la opción correcta con el color verde.**

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

* None of these options
* The default Compute Engine service account
* A student user belonging to the qwiklabs.net organization
* The external bad.actor.demo@gmail.com user

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

* The finding with the earlier event time
* None of these options
* The finding with the latest event time
* Both findings are genuine incidents

**Task 4. Access the findings in Cloud Logging**

In this task, you’ll access the events related to the Security Command Center findings in Cloud Logging.

1. In the Google Cloud console, in the **Navigation menu** (Navigation Menu icon) click **Logging > Logs Explorer**. The **Logs Explorer** page opens. (You may need to click **More Products** to expand the **Navigation menu** options and locate **Logging** under **Operations**.)

**Accedemos al apartado Logs Explores dentro de la sección Logging, para visualizar los eventos relacionados con el Centro de Seguridad de comandos.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Copy the following query into the **Query** builder at the top of the page:

protoPayload.authorizationInfo.permission="resourcemanager.projects.setIamPolicy"

protoPayload.methodName="InsertProjectOwnershipInvite"

This query filters the IAM logs.

**Copiamos la consulta que nos ofrece el enunciado en el apartado Query, para filtrar los logs de IAM.**

1. Click **Run query**. The query results should display on the **Query results** pane.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. In the **Query results** pane, expand the audit log listed for your project.
2. Click **Expand nested fields**. All the nested fields contained in the log are made visible.

**Abrimos el resultado de la consulta.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

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.

**Como podemos ver a continuación, nos muestra información como la autenticación (correo electrónico que se ha utilizado para asignar la cuenta externa); solicitud y metadatos (la cuenta externa que está provocando los problemas y la dirección IP donde se realizó la solicitud).**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

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

* A student user belonging to the qwiklabs.net organization
* A Google Cloud IAM service account
* An external @gmail.com account
* None of these options

**Task 5. Fix the finding**

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.

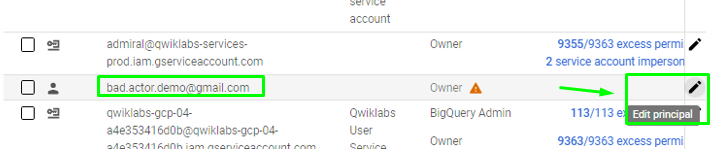
**Por último, entraremos al apartado IAM & Admin y quitaremos el permiso de Owner a la cuenta externa para solucionar los problemas provocados.**

1. In the Google Cloud console, in the **Navigation menu** (Navigation Menu icon), click **IAM & Admin** > **IAM**. The **IAM** page opens.

Interfaz de usuario gráfica

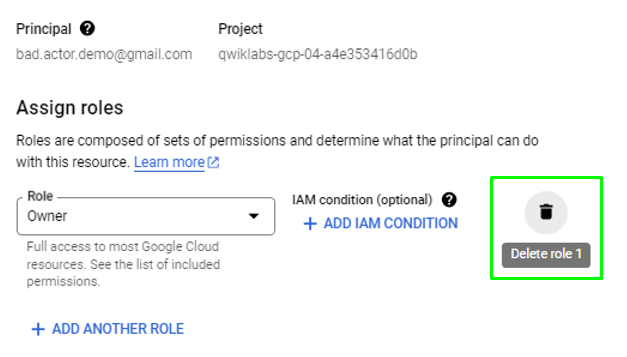
Descripción generada automáticamente

1. Next to the **bad.actor.demo@gmail.com** user, click the **Edit principal** (Edit icon) icon. The **Edit permissions** page opens.

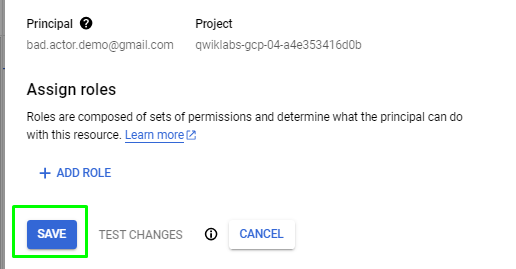


1. Click the **Delete** (Delete icon) icon to delete the owner role.

**Borramos el rol de propietario a la cuenta externa.**



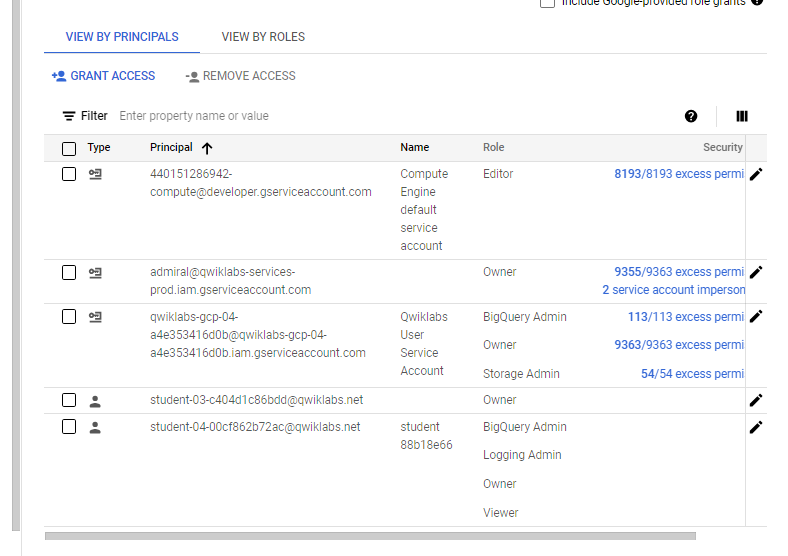
1. Click **Save**.



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

**Comprobación desde la consola de Google Cloud.**

**Ya no aparece la cuenta externa.**



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

|  |
| --- |
| Fix the finding  Check my progress |

Interfaz de usuario gráfica

Descripción generada automáticamente

**Conclusion**

Great work! Through this lab activity, you have gained practical experience in analyzing a security alert to determine whether it is a genuine malicious activity.

You did this by granting permissions to an external user, viewing the Event Threat Detection findings in the Security Command Center, and accessing the findings in Cloud Logging. Finally, you remediated the finding by removing the project owner role from the external user.

As a security analyst, these are skills that can enable you to quickly take steps to contain, mitigate, and remediate any threats.

**End your lab**

Before you **end the lab**, make sure you’re satisfied that you’ve completed all the tasks. When you're ready, click **End Lab** and then click **Submit**.

Ending the lab will remove your access to the lab environment, and you won’t be able to access the work you've completed in it again.

Copyright 2024 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.