****

P2 Explore false positives through incident detection

26 de junio de 2024

ADRIÁN GONZÁLEZ IGLESIAS

MÁSTER SISTEMAS MULTICLOUD

INSTITUTO TAJAMAR

**Índice**

Contenido

[**Índice** 1](#_Toc170206546)

[**Explore false positives through incident detection** 2](#_Toc170206547)

[**Activity overview** 2](#_Toc170206548)

[**Scenario** 3](#_Toc170206549)

[**Task 1. Create a service account** 4](#_Toc170206550)

[**Task 2. Create a JSON authentication key for your service account** 5](#_Toc170206551)

[**Task 3. Trigger the false positive finding** 7](#_Toc170206552)

[**Task 4. Sign in as the second user** 9](#_Toc170206553)

[**Task 5. View the threat finding in SCC** 10](#_Toc170206554)

[**Task 6. Fix the finding** 12](#_Toc170206555)

[**Conclusion** 13](#_Toc170206556)

[**End your lab** 13](#_Toc170206557)

**Explore false positives through incident detection**

[Explore false positives through incident detection | Google Cloud Skills Boost](https://www.cloudskillsboost.google/paths/419/course_templates/969/labs/485952)

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**

A **false positive** is an alert that incorrectly detects the presence of a threat. False positives can be triggered by genuine and legitimate user activity. Security teams may spend lots of time and resources investigating false positive alerts only to discover that there is no real threat.

In this lab, you'll recreate the activity that generates a false positive alert. Then, you'll access and analyze the false positive threat using Security Command Center (SCC) and take action to address it. You'll be using two separate accounts in this lab: one account to trigger the false positive and another account to analyze and remediate the false positive.

**Scenario**

Your team lead, Chloe, has been notified of a low severity security alert. The alert identified a service account with broad permissions using insecure key management practices through user managed keys. Upon further investigation it was found that Hank, the cloud architect, unintentionally triggered this alert. Hank was testing a new service account and accidentally created the key for the test user account. This alert was addressed and closed as a false positive.

Chloe believes this alert serves as a great example of a false positive alert. Chloe has tasked you with recreating the activity that triggered the false positive alert. You'll analyze the alert and then remediate it. The process of recreating the false positive serves as a valuable learning experience that will help you understand how and why the alert was triggered and how you can implement effective security policies to mitigate further false positive alerts.

Here's how you'll do this task: **First**, you'll recreate the false positive by creating a service account, assigning a role, providing a key, and activating the service account. **Then**, you'll use Security Command Center (SCC) to access the vulnerability finding related to activity you triggered. **Finally**, you'll take action to remediate the vulnerability finding and take action to remediate the false positive.

**Task 1. Create a service account**

***Note:****Make sure you are on the****username 1: Google Cloud username 1****Google Cloud console.*

In this task, you’ll create a service account and grant it permissions sufficient to trigger an anomalous threat finding in SCC.

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

**Accedemos al apartado Service Accounts dentro de IAM & Admin para crear una Service Account con la que activaremos el falso positivo asignando el rol de propietario.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. In the action bar, click **+ Create Service Account**.

**Entramos en Create Service Account.**

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

Descripción generada automáticamente

1. In the **Service account details** section:
   * In the **Service account name** field, type **test-account**.

Notice the **Service account ID** automatically populates.

**Asignamos el nombre test-account a nuestra cuenta.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

* + Click **Create and Continue**.

Notice the pop-up message “Service account created”.

**Dejamos los demás valores por defecto y continuamos con la configuración de la cuenta.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. In the **Grant this service account access to project** section, expand the **Select a role** drop-down menu, select **Basic**, and then select **Owner**.

**A continuación, en Select a role, seleccionamos acceso Basic y el rol de Owner.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click **Continue**, and then click **Done**.

**Pinchamos en continuar y en Done para finalizar la configuración.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Notice the **test-account** service account listed in the **Service accounts** list.

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

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

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

|  |
| --- |
| Create a service account  Check my progress |

Escala de tiempo

Descripción generada automáticamente con confianza media

**Task 2. Create a JSON authentication key for your service account**

***Note:****Make sure you are on the****username 1: Google Cloud username 1****Google Cloud console.*

In this task, you’ll create and download a JSON authentication key for the new service account you created in the previous task. You’ll then use Cloud Shell to upload that key to your Google Cloud account. This will trigger a threat finding in SCC.

**Lo siguiente que haremos será descargar una key tipo JSON para la nueva cuenta, de tal manera, que luego usaremos el Cloud Shell para cargar dicha clave en la cuenta. Con esto provocamos que se desencadene una amenaza en SCC (Security Command Center).**

1. Still on the **Service Accounts** page, inline with the **test-account** service account, click **Actions** (More Icon) **> Manage keys**. The **test-account** page opens.

**Accedemos a Manage Keys de nuestra cuenta recién creada.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. In the **Keys** section, click **Add Key > Create new key**.

**Entramos en Create new key.**

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

Descripción generada automáticamente

1. In the **Create private key** dialog, set the **Key type** to **JSON**.
2. Click **Create**.

**Queremos que sea tipo JSON como ya hemos nombrado antes.**

Imagen que contiene Correo electrónico

Descripción generada automáticamente

The console prompts you to download the key to your local device. Once downloaded, you’ll use Cloud Shell to upload the key to your Google Cloud (student) account.

**Comprobamos que al crear la key, se descarga automáticamente en nuestros archivos locales.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On your local device, navigate to the key file you just downloaded and rename it **test-account**.

**Renombramos el archive al nombre de nuestra cuenta creada anteriormente.**



1. In the Google Cloud console, click the Activate Cloud Shell (Cloudshell Icon) icon.

**Accedemos a la Cloud Shell en la parte superior de la consola de Google Cloud.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click **Continue**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

It should only take a few moments to provision and connect to the Cloud Shell environment.

1. In the Cloud Shell title bar, click **More** (More Icon) **> Upload > Choose Files**.

**Una vez dentro de la Cloud Shell, vamos a subir nuestra key, entrando en los 3 puntos – Upload.**

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

Descripción generada automáticamente

**Tipo File – Choose Files.**

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

Descripción generada automáticamente

1. Navigate to and select the file on your local machine, and then in the **Upload** dialog, click **Upload**.

**Seleccionamos nuestro archivo y lo subimos**

Diagrama

Descripción generada automáticamente

1. Copy the following command into the Cloud Shell terminal:

**Realizamos un ls para comprobar que se ha agregado correctamente.**

ls

This command lists the key file you just uploaded.

1. Press **ENTER**.

Texto

Descripción generada automáticamente

In the **test-account** page, in the **Key** list, notice the key you just created with the **Key creation date** as the current date.

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

Texto

Descripción generada automáticamente

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

|  |
| --- |
| Create a JSON authentication key for your service account  Check my progress |

Create a JSON authentication key for your service account

Check my progress

Escala de tiempo

Descripción generada automáticamente

**Task 3. Trigger the false positive finding**

***Note:****Make sure you are on the****username 1: Google Cloud username 1****Google Cloud console.*

In this task, you’ll reconfigure the Cloud Shell environment to use the new **test-account** service account that you created in Task 1. This will trigger a threat finding in SCC. Then, you’ll assign excessive permissions to the lab project.

**Lo siguiente que realizaremos será, usar la nueva cuenta de servicio que creamos en el anterior Task. Con estos conseguimos, al igual que antes, volver a desencadenar una amenaza.**

1. Copy the following command into the Cloud Shell terminal:

**Añadimos estos comandos al Cloud Shell para activar la nueva cuenta.**

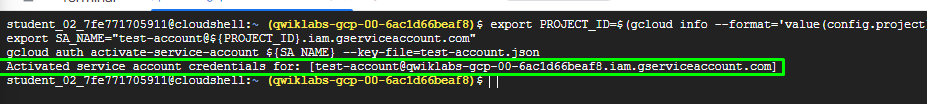
export PROJECT\_ID=$(gcloud info --format='value(config.project)')

export SA\_NAME="test-account@${PROJECT\_ID}.iam.gserviceaccount.com"

gcloud auth activate-service-account ${SA\_NAME} --key-file=test-account.json

This command activates the new service account.

1. Press **ENTER**.



1. Copy the following command into the Cloud Shell terminal:

**Agregamos el comando gcloud auth list, para comprobar que se ha activado correctamente.**

gcloud auth list

This command confirms that you activated the service account, and that gcloud is using this service account.

1. Press **ENTER**.

Texto

Descripción generada automáticamente

1. Copy the following command into the Cloud Shell terminal:

**El siguiente comando nos permitirá asignar el rol de editor al usuario, para poder corregir la amenaza del falso positivo.**

export STUDENT2="Google Cloud username 2"

gcloud projects add-iam-policy-binding $PROJECT\_ID --member user:$STUDENT2 --role roles/editor

This command grants the editor role to user 2 so that you can access and remediate the false positive finding in the next task.

1. Press **ENTER**.

Texto

Descripción generada automáticamente

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

|  |
| --- |
| Assign excessive permissions to trigger threat detection  Check my progress |

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Task 4. Sign in as the second user**

You'll need to switch Google Cloud accounts by logging into the Google Cloud console using the second user account provided in the **Lab Details** panel. You will use this user account to perform the remaining tasks.

**A continuación, añadiremos la segunda cuenta de usuario que nos proporciona el laboratorio, que será la encargada de visualizar las siguientes tareas.**

1. In the Google Cloud console, click on the user icon in the top-right corner of the screen, and then click **Add account**.

**Entramos en Add account en la parte superior derecha de la consola de Google Cloud.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Navigate back to the **Lab Details** panel, copy the **Google Cloud username 2**: Google Cloud username 2 and **password**. Then, paste the username and password into the Google Cloud console **Sign in** dialog.

**Copiamos el nombre de usuario en la interfaz del laboratorio.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Pegamos el nombre en el inicio de sesión, con su respectiva contraseña.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Task 5. View the threat finding in SCC**

***Note:****Make sure you are on the****username 2: Google Cloud username 2****Google Cloud console.*

In this task, you’ll locate and examine the SCC finding generated by the service Event Threat Detection. This finding is a false positive that was triggered by the activity you generated in Tasks 1-3.

**Vamos a localizar y entender la amenaza desencadenada en los anteriores Tasks, asegurándonos que estamos con la cuenta de usuario 2.**

To view the Event Threat Detection finding in SCC:

1. In the **Navigation menu** (Navigation Menu icon), click **Security > Findings**.

**Accedemos a Findings dentro de Security.**

Imagen que contiene Diagrama

Descripción generada automáticamente

1. In the **Quick filters** pane, locate the **Category** section, then select **User managed service account key**. If necessary, click **View more** to find it.

**En la sección Quick filters, marcamos la opción User managed service account key, que es la que nos corresponde para este apartado.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

The **Findings query results** panel updates to display only the selected finding category.

1. In the **Findings query results** panel, display the details of the finding by clicking the most recent (see **Event time**) **User managed service account key** in the **Category** column. The details panel for the finding opens and displays the **Summary** tab.

**Si vamos un poco más a la derecha, podemos ver la hora actualizada de la amenaza provocada.**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Leave the **User managed service account key** page open to answer the following questions.

1. What is the severity of the alert?

* Critical
* Medium

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

* High
* Low

2. What is the threat finding class for the alert?

* Vulnerability
* Threat
* Misconfiguration

Texto

Descripción generada automáticamente con confianza baja

* Observation

3. When is it important to monitor for threats?

* Whenever you access the corporate network on your tablet or smartphone
* Whenever your device is on
* Whenever you device is on site
* Whenever your device is connected to the internet

4. Which tab in the **User managed service account key** page provides compliance standards, explanation of the threat, and a recommendation on how to handle the threat?

* Summary
* Source Properties
* JSON

**Task 6. Fix the finding**

***Note:****Make sure you are on the****username 2: Google Cloud username 2****Google Cloud console.*

In this task, you'll remediate the false positive by deleting the JSON authentication key for the **test-account** service account.

**Por último, vamos a eliminar la Key para solucionar el falso positivo.**

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

**Accedemos de nuevo a Service Accounts.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. On the **Service accounts** page, click the email address of the **test-account** service account.

**Entramos en la Service Account que hemos utilizado.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Click the **Keys** tab.

**Entramos en Keys.**

Diagrama

Descripción generada automáticamente con confianza media

1. From the list of keys, click the **Delete service account key** (Delete Icon) icon to delete the key. A pop-up will appear asking you to confirm the action. Click **Delete**.

**Pinchamos en Delete de la Key que hemos creado.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Como podemos ver en la consola de Google Cloud, ya no tenemos ninguna Key.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

|  |
| --- |
| Delete the key  Check my progress |

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Conclusion**

Great work!

You have completed this lab! You used SCC to investigate a false positive and took action to remediate it. As a cloud security analyst, you'll likely encounter false positive alerts. It's important to understand how and why false positive alerts are triggered and how you can take action to remediate them.

**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.