EVENT THREAT DETECTION USING SCC

PROJECT DESCRIPTION

In this Lab, I analyzed findings in the Google Cloud Security Command Center (SCC) and examined related events in Cloud logging.

SCENARIO

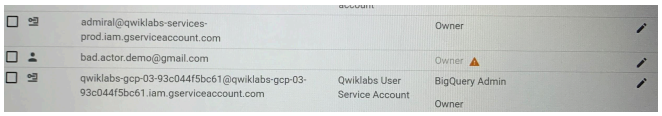
The Security team discovered two threat findings relating to suspicious activity with user accounts. The threat findings were promptly investigated and remediated. One of the findings was determined to be benign user activity while the other finding was confirmed as malicious. I was tasked with examining the details behind each finding so that I can understand the difference between normal activity and malicious activity.

Here's how I did this ;

First step: Grant Permissions To An External Account

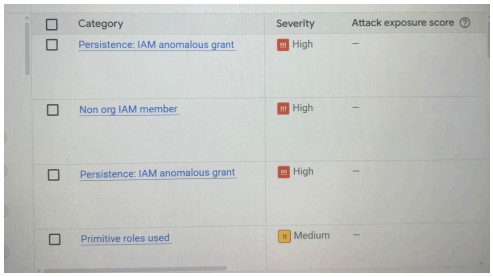
I granted project owner rights to an external gmail account. Granting owner rights to an external account will trigger the Event Threat Detection IAM detectors. Aside from the external account, a user is listed in the **labs details** panel as student-02-5a7737389665@qwiklabs.net . This user has automatically been granted **owner** roles to the lab project. This triggered an alert finding or incident because an external principal has an owner role. However, since the user belongs to qwiklabs.net I considered it **"normal activity".**

I now have 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.



Second step: Access The Event Threat Detection Findings

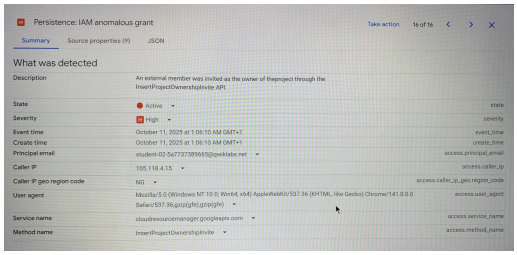
I accessed the Event Threat Detection Findings in the SCC. I noticed three findings with high severity listed in the **"Finding query results"** panel**.** I examined two **persistence: IAM anomalous grant** findings to determine whether the finding is normal activity or whether it is malicious.



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 my environment.
Next, I filtered the findings to display a list of Persistence: IAM anomalous grant category findings
The filter returns two **persistence: IAM anomalous grant** findings.
Then I sort the findings in descending order, so that the earliest finding is at the top.

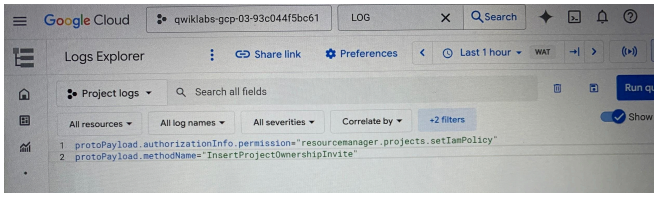
Third step: Analyze The Findings
I examined these findings to determine which is normal activity and which is a genuine incident.
The **Persistence: IAM Anomalous Grant** dialog opens on the **summary** tab, which displays the finding summary.



The **principal email** row, which happens to be the user account mentioned in the **first step** that “granted the owner role to the user”. Since this service account belongs to the qwiklabs.net I established that this finding represents **Normal and Expected Activity.**
Next I located the malicious activity associated with the external user account I had granted access to : **bad.actor.demo@gmail.com**
The value on the **principal email** row shows this is the user account email address that granted the owner role to the user. With this information, I established that this finding is associated with an **Unauthorized and malicious actor.**

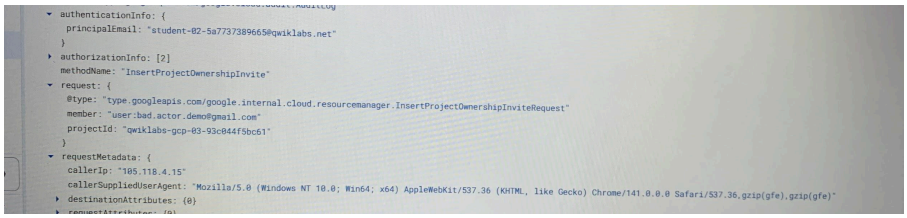
Fourth Step: Access The Finding In Cloud Logging
I accessed the events related to the SCC findings in Cloud logging.
The following **Query** was typed into the **Query builder ;**

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



This query filters the IAM logs.
I then examined 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.



Final Step: Fix The Finding
I remediated the malicious **Persistence: IAM Anomalous Grant** finding by removing the project owner role that I had previously assigned to the external user.
The policy is then updated and the owner role removed from the **bad.actor.demo@gmail.com** user.

CONCLUSION
Through this lab activity I gained practical experience in analyzing a security alert to determine whether it is a genuine malicious activity.
I did this by granting permissions to an external user, viewing the Event Threat Detection findings in the SCC and accessing the findings in cloud logging. Finally I remediated the finding by removing the project owner role from the external user.
As a security analyst, these are the skills that can enable me to quickly take steps to contain, mitigate and remediate any threats.