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

Scenario

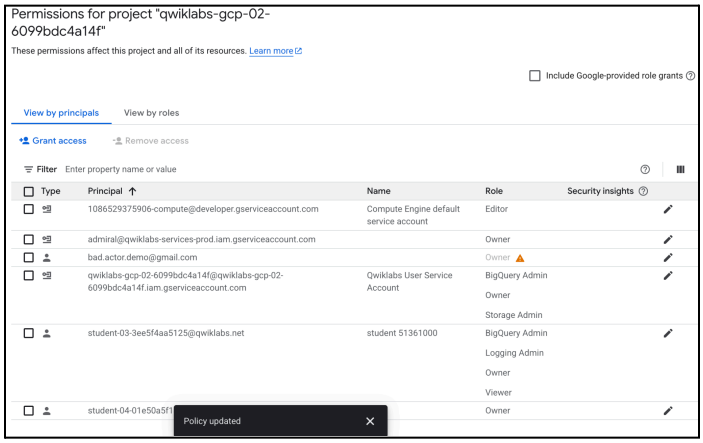
Recently, the security team discovered two threat findings relating to suspicious activity with user accounts. The threat findings were promptly investigated and remediated. One of the findings was determined to be benign user activity while the other finding was confirmed as malicious. Your team lead, 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.

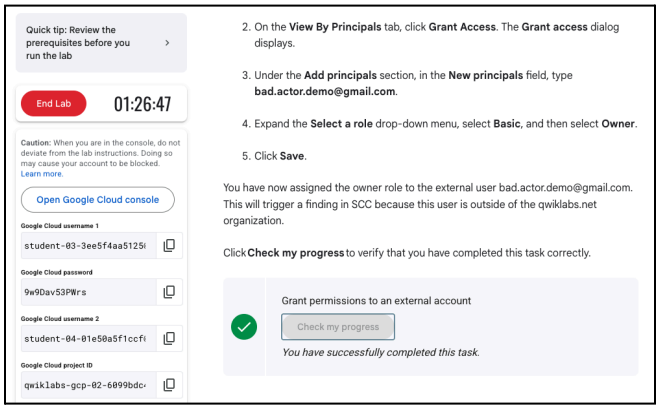
Here's how you'll do this task: **First**, you'll grant permissions to an external account to trigger an Event Threat Detection IAM finding. **Then**, you'll use the Security Command Center to access the two IAM findings. **Next**, you'll analyze details of the findings using Security Command Center 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

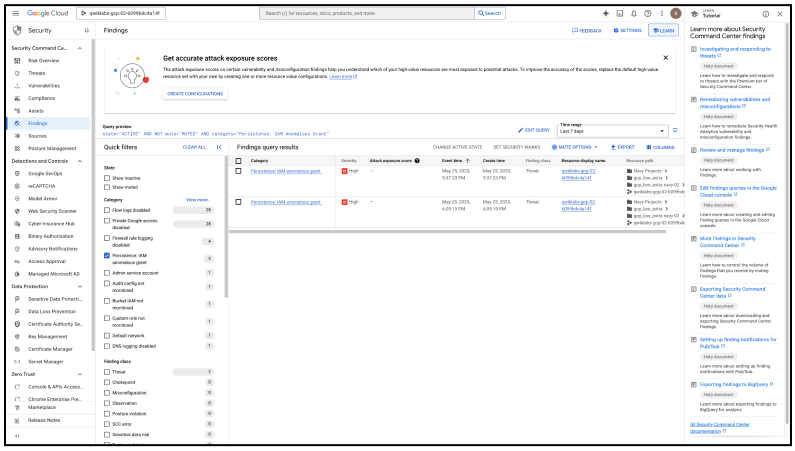
In this lab, the focus is to determine the difference between normal activity and an incident. In this task, I granted permission to an external account in order to learn the difference.





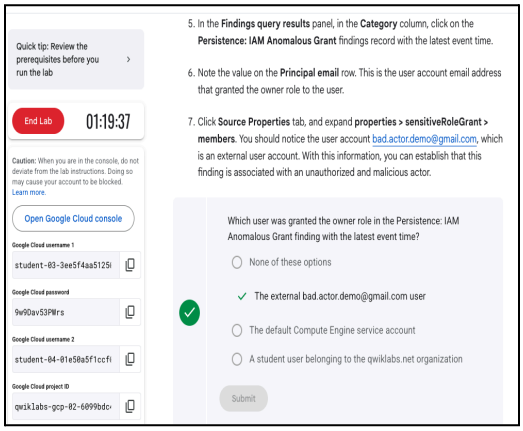
Task 2: Access the Event Threat Detection findings

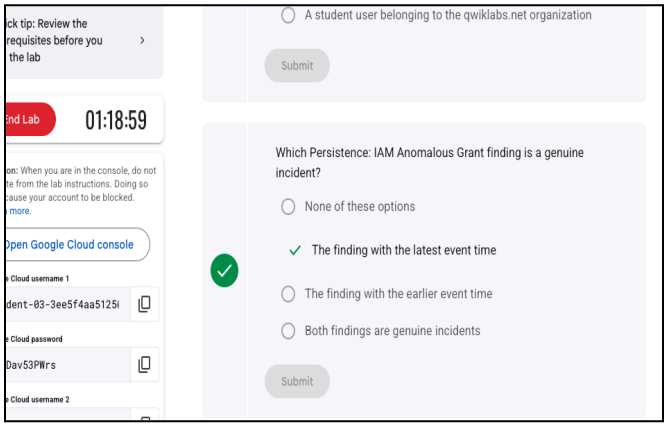
In this task, an anomalous grant was detected with a high severity.

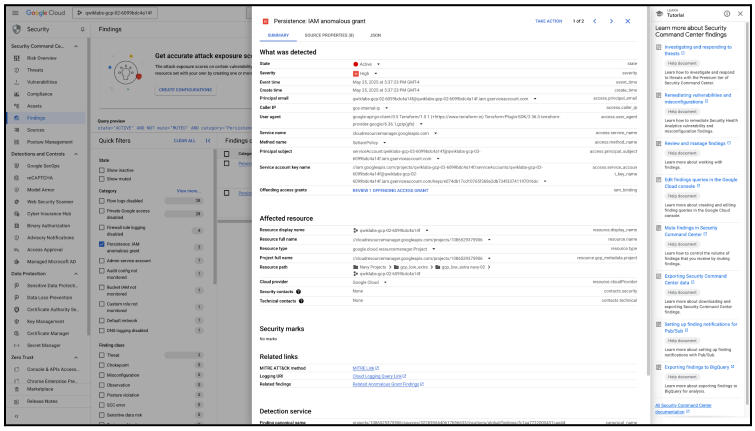


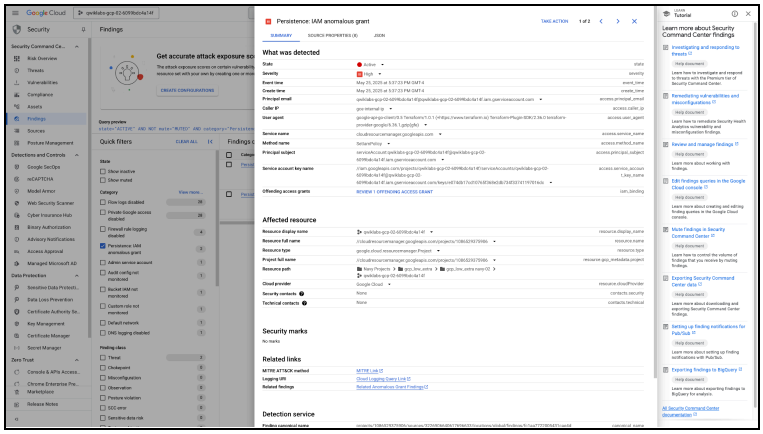
Task 3: Analyze the findings

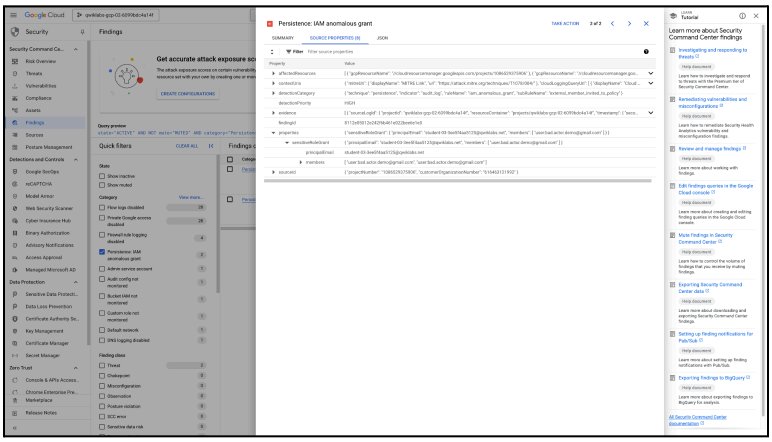
In this task, I reviewed the findings to determine which account was genuine versus which was an incident.





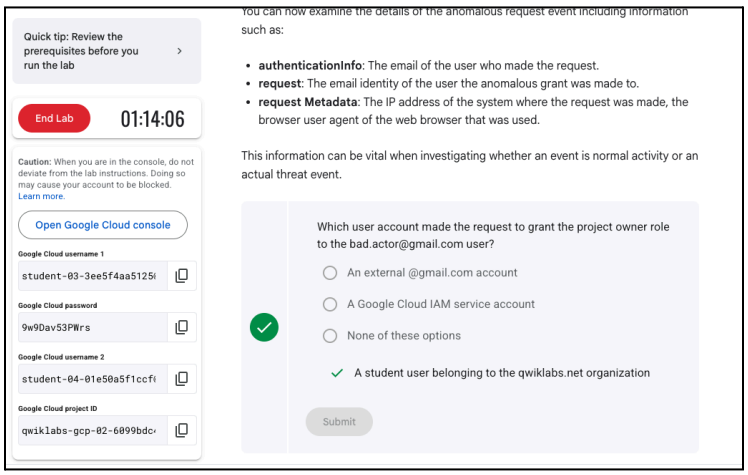


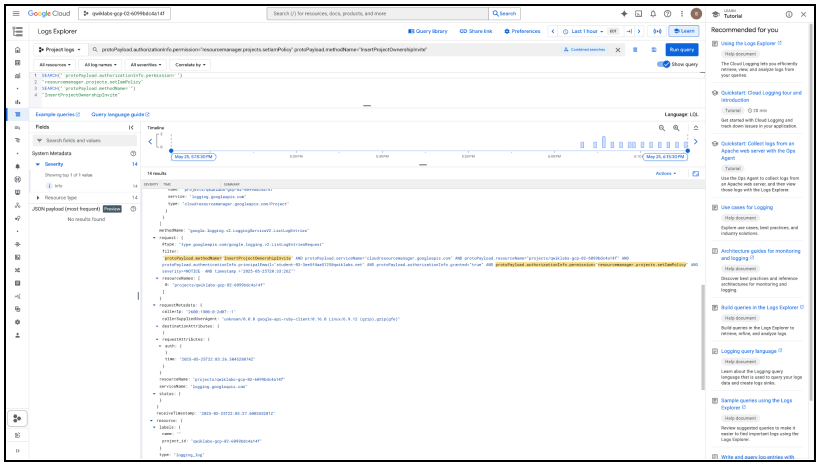




Task 4: Access the findings in Cloud Logging

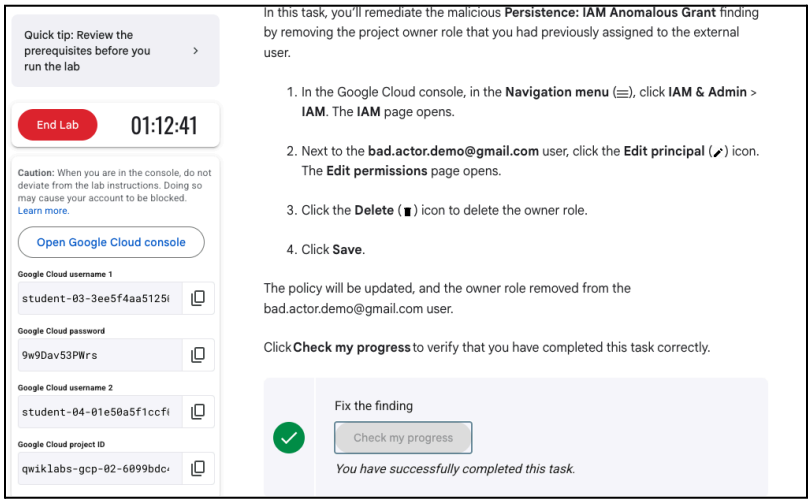
In this task, I was able to use Logs Explorer and run a query to determine who granted access to the suspicious user.





Task 5: Fix the finding

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



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.