THREAT: Persistence: New API Method

Explanation:

GCP SCC Detects when a new API method has been called in the last 30 days.

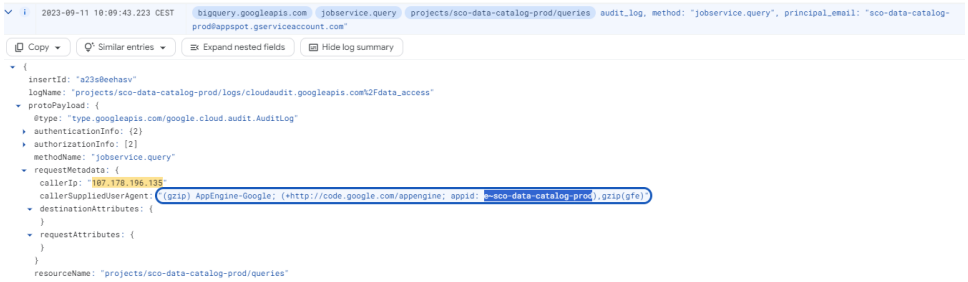
Resolution:

Investigation is required to understand if the API is called by a Solvay's Trusted source (within Solvay's network or cloud resources).

This threat cannot be easily mitigated. Further investigation is required to ensure the action is expected.

This can be either an expected or unexpected action.
The GCP Security team will need to evaluate based on the actions below:

Actions	Follow up
Check if the API call is successful or not	**Not successful** - End the investigation with expected action in the next table. **Successful** - Continue with the next action below.

Check if the IP comes from solvay.com's resources.
 	
How to check:
 	
• IP belongs to Solvay network.
• IP belongs to GAE within Solvay's organization.
  ○ To know if IP belongs to Solvay's GAE:
  ▪ Go to the GCP project of the reported finding.
  ▪ Check on the logs based on this IP. (See below for example of the GAE, with project code of the calling GAE, was called)
 
	Yes - End the investigation with expected action in the next table.
	
	No - Continue with the next action below.

Check if the new API method has no name	**No name for API** - End the investigation with expected action in the next table due to fault report. **Has name for API** - Continue with the next action below.
Check if the project belongs to Production	**Not production -** End the investigation with expected action in the next table. Non-production environment will be used by developers to test new API methods. **Production -** Continue with the next action below.

Check with owner/technical team on the usage of new API	**Expected** - End the investigation with expected action in the next table. **Unexpected** - End the investigation with unexpected action in the next table.

See the table below for recommended action after investigation.

Yes / No	Action
Yes, it is expected	Update the JIRA ticket to be "False positive - Expected action from the service account".
No, it is **not** expected	Further investigation is needed to remove the invoked command for this service account. If it is not invoked from a known procedure, the service account is most likely compromised. 1. Replaced with a new generated json key for the service acount. 2. Report this incident to the Solvay Security Operation team.

Pattern:

```
{
        "newApiMethod": {
                "newApiMethod": {
                        "serviceName": "compute.googleapis.com",
                        "methodName": "v1.compute.projects.setCommonInstanceMetadata"
                },
                "principalEmail": "xx-xxx@xx.iam.gserviceaccount.com",
                "callerIp": "xx.xx.xx.xx",
                "callerUserAgent": "(gzip),gzip(gfe)",
                "resourceContainer": "projects/xxx"
        }
}
```