Threats - Persistence: New User Agent

Explanation:

GCP SCC detect new user agent that access to the GCP project.

*User Agent:

In computing, a user agent is any software, acting on behalf of a user, which "retrieves, renders and facilitates end-user interaction with Web content." A user agent is therefore a special kind of software agent. Some prominent examples of user agents are web browsers and email readers.

Resolution:

Further investigation is required to see which action to be performed.

The GCP Security team will need to evaluate based on the actions below:

Actions	Follow up
Check if the environment belongs to Production. This is based on the assumption that all non-production enviroment should not contain production data and developer can be performing testing.	**Production** - Proceed to the next verification. **Non-Production** - Don't have to inform application owner and update to be false positive.
Check if the callerIp belongs to Solvay's IP.	**Solvay's IP** - Don't have to inform application owner and update to be false positive. **Not Solvay's IP** - Proceed to verify with application owner.

Verify if the reported user agent is valid and used by the principal email.

If is not, it could mean that hacker is trying to access to this resource.

Yes / No	Action
Yes, it is a valid access	Update the JIRA ticket to be false positive.
No, it is **not** a valid access	The principal email could be compromised. Revoke the permission from GCP IAM and escalate to the ***security operation team**.

Pattern:

```
{
        "anomalousSoftware": {
                "anomalousSoftwareClassification": ["firebase-cli"],
                "callerUserAgent": "FirebaseCLI/7.4.0,gzip(gfe)",
                "principalEmail": "xx@xx.com",
                "notSeenInLast": "2592000s",
                "typicalUserAgents": ["gcloud"],
                "rawUserAgent": "FirebaseCLI/7.4.0,gzip(gfe)",
                "callerIp": "xx.xx.xx.xx"
        }
}
```