THREAT: Persistence: Service Account Key Created

Explanation:

GCP SCC detects that a new Service Account .

This alert is regarding the creation of key for the service account which the application owner might not be awared of.

The **application owner will need to be informed to decide if any actions are required**.

Currently, only on **Production** environment will require to inform the application owner.

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. **Exceptions** If the user is the application owner, then there is no need to inform.	**Production** - Inform owner **Non-Production** - Don't have to inform owner.

See the table below for recommended action after investigation.

Yes / No	Action
Inform owner.	Inform the owner about the activity and update the JIRA ticket's rememdiation action to be "Owner is being informed" and closed the ticket.
Don't have to inform owner.	Update the JIRA ticket's rememdiation action to be "Non-production environment. No action to be taken." and closed the ticket.

Pattern:

```
{
        "principalEmail": "xxx@solvay.com",
        "callerIp": "xx.xx.xx.xx",
        "callerIpGeo": {
                "regionCode": "xx"
        },
        "serviceName": "iam.googleapis.com",
        "methodName": "google.iam.admin.v1.CreateServiceAccountKey",
        "principalSubject": "user:xxx@solvay.com",
        "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/121.0.0.0 Safari/537.36,gzip(gfe)"
}
```