

# Threats - Persistence: New Geography

## Explanation:

GCP SCC detect new geographical location which try to access the target GCP resource.

For this example:

[xx@xxx.com](#) is usually accessing from "US". It is detected that this principal email is now accessing from FR.

## Resolution:

Verify if the reported principal email is indeed coming for the reported location.

Advice them on the following:

- Always use Solvay VPN when travelling.
- Make sure they are using Looker Studio to access resources in the reported project.
  - If they are using Looker Studio, please get the user to change the connection using GSA. See this [page](#) for more information.
- If they confirmed they are not the one and they are not using Data/Looker Studio, reset their password.

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 <b>not</b> a valid access | The principal email could be compromised.<br>Ask reported users to change their passwords.<br>Update the JIRA ticket to be "Informed user". |

If the reported principal email belongs to a Google Service Account (GSA), please refer to the following:

| Prod / Non-Prod                                                                                                       | Action                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If GSA name starts with " <b>sa-looker-</b> ", this is service account created to be used by Looker Studio Dashboard. | Update the JIRA ticket to be false positive.<br>Reason is the GSA is used for Looker Studio Dashboard.                                                                                                                                                                                                                                                        |
| Non-Prod                                                                                                              | Update the JIRA ticket to be false positive.<br>Reason is the environment is non-production.<br>Developers are using GSA for individual testing.                                                                                                                                                                                                              |
| Prod, within Solvay's IP                                                                                              | Update the JIRA ticket to be false positive.<br>Reason is the Solvay's application is using this GSA to access production data.                                                                                                                                                                                                                               |
| Prod, <b>NOT</b> within Solvay's IP                                                                                   | Inform the application owner about the access to production with GSA done by individuals.<br><br>This might be a case that someone outside of Solvay connecting to Production data.<br><br><b>Recommendation:</b> Application Owner to investigate and rotate the GSA key for this service account to avoid further potential compromised to production data. |

## Pattern:

```
{
  "anomalousLocation": {
    "anomalousLocation": "FR",
    "callerIp": "xx.xx.xx.xx",
    "principalEmail": "xx@xxx.com",
    "notSeenInLast": "2592000s",
    "typicalGeolocations": [{
      "country": {
        "identifier": "US"
      }
    }]
  }
}
```

## More Information:

Problem when you use your own account for solution such as Data Studio: