THREAT: Exfiltration: BigQuery Data Extraction

Explanation:

GCP SCC detects that BigQuery Data has been exported.

This alert is regarding the extraction of data from Bigquery and it is to keep the application owner aware of the action.
[Safeguarding Solvay's Data]

The data within the Bigquery might be sensitive and it is not possible for CloudOps to make any decision.
Therefore 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. This is based on the assumption that all non-production enviroment should not contain production data. **Exceptions** If project is under "Revevol-Solvay" folder within the GCP and the alerted user accounts are under Revevol • Close finding with "False positive. Revevol is authorized for action in this project."	**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:

```
{
        "extractionAttempt": {
                "job": {
                        "projectId": "xxx",
                        "jobId": "xxx",
                        "location": "xx"
                },
                "jobLink": "https://console.cloud.google.com/bigquery?j=bq:EU:
xxx&project=xxx&page=queryresults",
                "sourceTable": {
                        "projectId": "xxx",
                        "datasetId": "_6dfcf38d2e4871bc0f28db275bdb846a85949f11",
                        "tableId": "anon955db38d_b8ae_4c41_9b9d_225df2d76950",
                        "resourceUri": "projects/xxx/datasets/xxx/tables/xxx"
                },
                "destinations": [{
                                "originalUri": "gs://xx/report-bigquery/report-CSV-05-04-2022_16:36:57.csv",
                                "collectionType": "GCS_BUCKET",
                                "collectionName": "xxx",
                                "objectName": "report-bigquery/report-CSV-05-04-2022_16:36:57.csv"
                        }
                ]
        },
        "principalEmail": "xxx@xxx.iam.gserviceaccount.com"
}
```