THREAT: Initial Access: Dormant Service Account Action

Explanation:

Detects events where a dormant user-managed service account triggered an action. In this context, a service account is considered dormant if it has been inactive for more than 180 days.

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:

<table>
<tr><th>Actions</th><th>Follow up</th></tr>
<tr><td>Open the Initial Access: Dormant Service Account Action finding, as directed in Reviewing findings.
In the finding details, on the Summary tab, note the values of following fields.

Under What was detected:

• Principal email: the dormant service account that performed the action
• Service name: the name of the service involved in the action
• Method name: the method that was called

Check with the application owner that the service account in the Principal email field whether the legitimate owner conducted the action.

<table><tr><th>Exceptions</th></tr><tr><td>For Service acount with "pipeline" and "terraform@xxx" naming is used for pipeline deployment. If the service name/method name is related to deployment, they can be exception.

Some deployments can happened more than 180 days.</td></tr></table></td><td>If not exception - Inform application owner

Exception case - Don't have to inform application owner.</td></tr>
</table>

See the table below for recommended action after investigation.

Yes / No	Action
Inform application 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 application owner.	Update the JIRA ticket's rememdiation action to be "False positive. Triggered by pipeline." and closed the ticket.