**GCP Logs flow to IBM QRadar**

**Introduction**

We should be sending audit logs

**Architecture** –

Diagram

Description automatically generated

**Audit Logs**

Audit logs are very important because they keep track of the user/service account activity across all gcp services. They can be referred to track the nature of the user activity.

There are below types of Audit logs –

* Admin Activity audit logs (Mandatory)
* Data Access audit logs (Mandatory)
* System Event audit logs (Mandatory)
* Policy Denied audit logs (Mandatory)

The Qradar team mentioned that these logs are in large volume. That's because these include read, list, write, update, delete actions. We can write filters to exclude read and list actions to reduce the volume of this data.

**Note**: Data access audit logs will be by default enabled for only BigQuery if project has need to use any other database then they should enable data access logs for that GCP service.

**VPC Flow Logs**

VPC flow logs keep track of all the activity that's been happening in a VPC between the resources like vm instances. Since there can be a lot of instances running in the VPC and they communicate all the time, the volume of these logs is very high.

Main purpose of these logs is troubleshooting and debugging the connectivity.

We can refrain from ingesting these logs into qradar instead they can be stored in GCS bucket for longer retention periods(compliance purpose)