GSuite Monitoring Solution (Google Reporting) integration with Threat Intelligence Platform

Login | Admin | Google Drive | Google Mail

Gsuite Reporting Logs

2. Customer Connector app makes call to Google Admin SDK Reporting API's to retrieve the log data based on input parameters by the User

1. Customer will display the configuration screen to User where User will enter the search Ctiteria (such as UserKey, ApplicationName, EventName, Filters etc.) to generate the required report

Customer Console

Customer Connector App

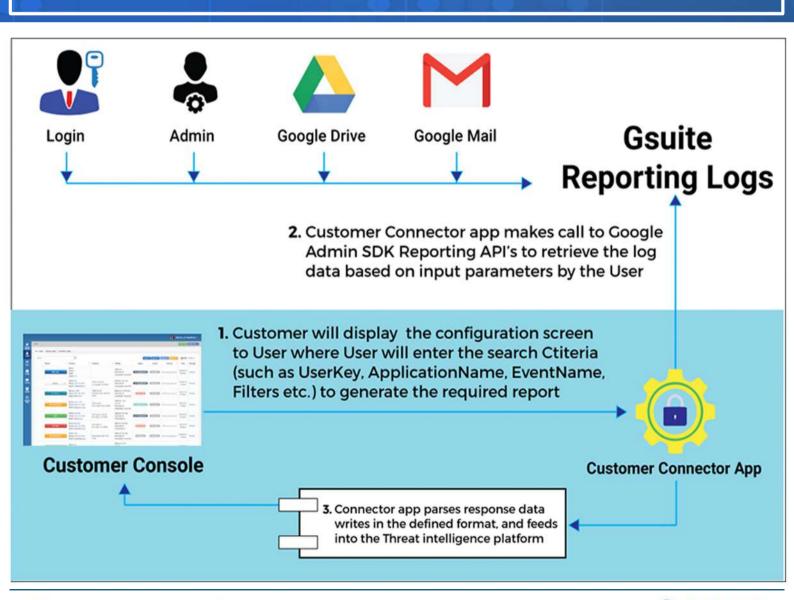3. Connector app parses response data writes in the defined format, and feeds into the Threat intelligence platform

Customer

Customer is a leading Threat Intelligence solution provider.

They provide a platform for companies to aggregate and act upon Threat Intelligence.

Customer requested for the integration of their product with the GSuite Monitoring solution

Requirement

Technology Solution

- Google provides the Reporting APIs to retrieve the logs based on certain criteria such as GuserKey, applicationName, eventName, startTime etc.
- Developed the front end app too get the search criteria
- Developed the Connector app to make call to Google Admin SDK Reporting APIs to retrieve the log data based on input parameters by the User
- Connector app parses response data and writes in the customer event format
- Selenium automation scripts were used to generate the GSuite events for testing