NG SIEM - GoogleWorkspace Integration

Introduction

The Google Workspace integration collects and parses data from various **Google Workspace audit reports APIs** using a service account authorized via the **Admin SDK API**.

Requirements

To ingest data from the Google Reports API, the following must be completed:

- An **administrator account** in Google Workspace.
- Enable the **Admin SDK API** in GCP.
- Create and configure a **Service Account**.
- Enable **Domain-Wide Delegation** for the service account.
- Configure the **OAuth Consent Screen**.

> Note this is only applicable for Administrator Account in Google Workspace. Thank you and have a nice day.

Enable Admin SDK API

Complete the following steps:

- Select the Google Cloud navigation menu > **APIs & Services** > **Enabled APIs & Services**
- Search and enable "**Admin SDK API**" from the **API library page**

Configure OAuth Consent Screen

Complete the following steps:

- Select the Google Cloud navigation menu > **APIs & Services** > **Enabled APIs & Services** > **OAuth Consent Screen**
- User Type > Internal > Create
- Fill out the following information in subsequent steps
- App name:
- User support email:
- Authorized domains:

- Developer contact information:
- Save and Continue
- Save and Continue
- Back to Dashboard

Create a Service Account

To create a service account, do the following:

- Select the navigation menu in Google Cloud > **APIs & Services** > **Credentials** > **Create Credentials** > **Service Account**
- Enter the following information:
- Service account name: a
- Service account ID:
- Leave the rest blank and continue
- Select your new **Service Account** > **Keys** > **Add Key** > **Create New Key** > **JSON**

Enable Domain-wide Delegation

- In your GW Admin Console select > **Navigation Menu** > **Security** > **Access and data control** > **API controls**
- Select **Manage Domain Wide Delegation** > **Add New**
- Client ID: OAuth ID from Service Account in GCP
- Google Cloud Console > **IAM & Admin** > **Service Accounts** > **OAuth 2 Client ID** (copy to clipboard)
- **OAuth Scopes**: https://www.googleapis.com/auth/admin.reports.audit.readonly

> Please provide the following information to CyTech Support. Thank you

- **Delegated Account -** the email of the administrator account, and not the email of the ServiceAccount.
- **Jwt JSON** - The JSON credentials file downloaded from GCP. Raw contents of the JWT file. Useful when hosting a file along with the agent is not possible. NOTE: Please use either JWT File or JWT JSON parameter.

Reference link: https://www.elastic.co/security-labs/google-workspace-attack-surface-part-two

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #6
Created 23 September 2025 08:10:51 by Richmond Abella
Updated 3 December 2025 07:18:40