# Google Cloud Platform (GCP) Audit Logs Integration - using Pub/Sub

## Requirements

To integrate with Google Cloud Platform (GCP), you need to set up the following:

1. **Service Account with a Role.**
2. **Service Account Key to access data on your GCP project.**

## Service Accounts

A **Service Account (SA)** is a special type of Google account intended for applications or services—not human users—that need access to GCP resources.

The **Log Collector** uses this SA to access GCP data via Google APIs.

## Service Account with a Role

Assign the necessary privileges by creating a **custom role** with minimal required permissions:

## Required Permissions:

- **compute.instances.list** (required for GCP Compute instance metadata collection) (**2)
- **monitoring.metricDescriptors.list**
- **monitoring.timeSeries.list**
- **pubsub.subscriptions.consume**
- **pubsub.subscriptions.create** (*1)
- **pubsub.subscriptions.get**
- **pubsub.topics.attachSubscription** (*1)

> **1 Only required if Agent is expected to create a new subscription. If you create the subscriptions yourself, you may omit these privileges.*

> ***2 Only required if corresponding collection will be enabled.*

>

> **After you have created the custom role, assign the role to your service account.**

## Service Account Key

Next, with the Service Account (SA) with access to Google Cloud Platform (GCP) resources setup, you need some credentials to associate with it: a Service Account Key.

From the list of SA (Service Accounts):

1. Go to **IAM & Admin > Service Accounts** in the GCP Console.
2. Click the service account you created.
3. Under the **"Keys"** section, click **"Add Key" > "Create new key"**.
4. Choose **JSON** as the key type.
5. **Download and securely store** the generated private key (it cannot be retrieved again from GCP if lost).

## GCP Integrations Procedures - GCP Audit Logs

The audit dataset collects audit logs of administrative activities and accesses within your Google Cloud resources.

### Procedures

The "Project Id" and the "Credentials File" will need to be provided in the integration UI when adding the Google Cloud Platform integration.

## Logs Collection Configuration

With a properly configured Service Account and the integration setting in place, it’s time to start collecting some logs.

### Requirements

You need to create a few dedicated Google Cloud resources before starting, in detail:

1. **Log Sink**
2. **Pub/Sub Topic**
3. **Subscription**

> It’s recommended to have a separate Pub/Sub topics for each of the log types so that they can be parsed and stored in a specific data stream.

Here’s an example of collecting Audit Logs using a Pub/Sub topic, a subscription, and a Log Router. We will create the resources in the Google Cloud Console and then configure the Google Cloud Platform integration.

## Example Setup Using Google Cloud Console

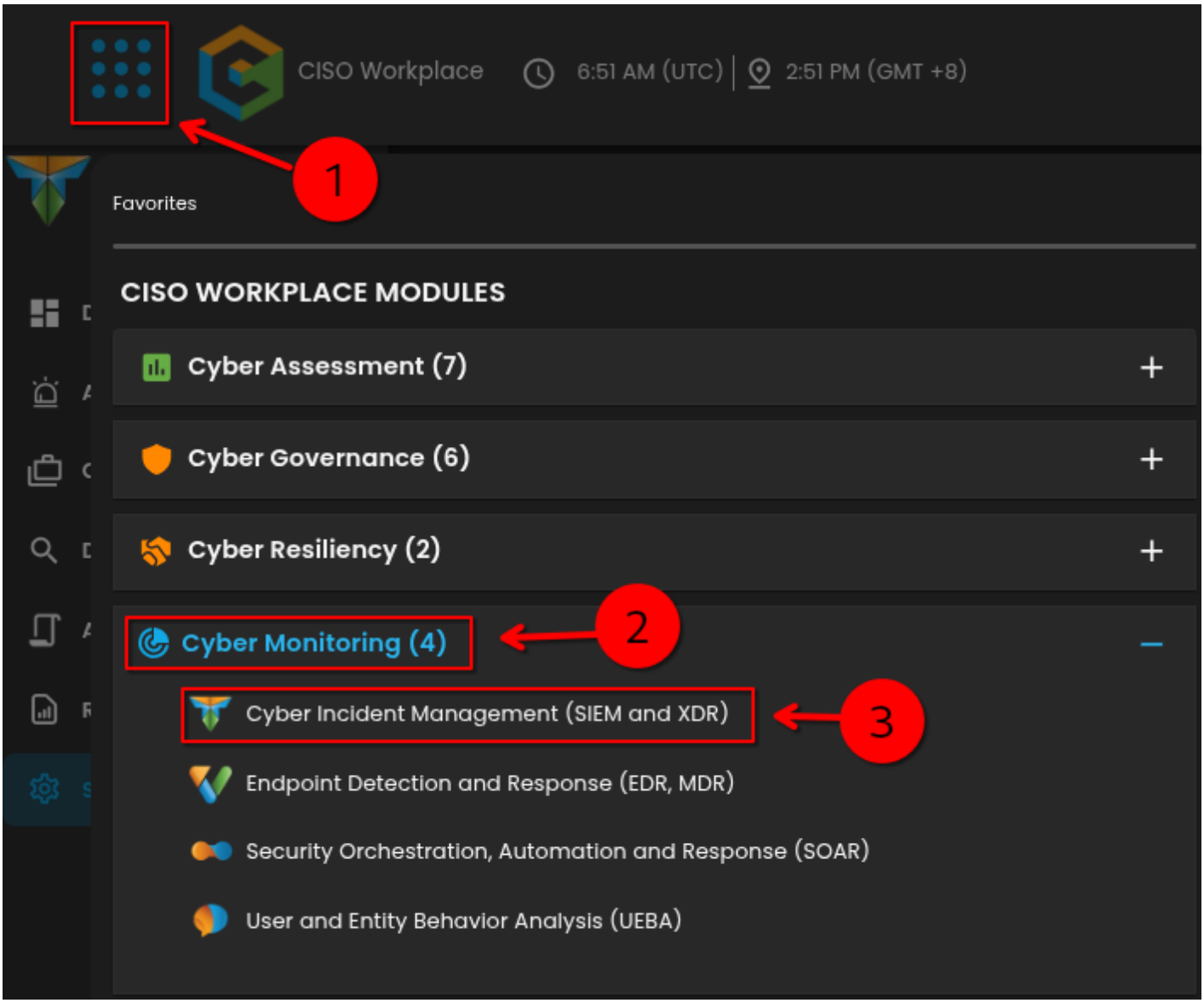
1. Navigate to **"Logging" > "Log Router" > "Create Sink"**.
2. Provide a **Sink name** and description.
3. For **Sink destination**, select **"Cloud Pub/Sub topic"**. Choose an existing topic or create a new one.
4. If a new topic is created, you must also **create a subscription** for it.
5. Under **"Choose logs to include in sink"**, use a filter like: logName:"cloudaudit.googleapis.com"

**Please provide the following information to CyTech:**

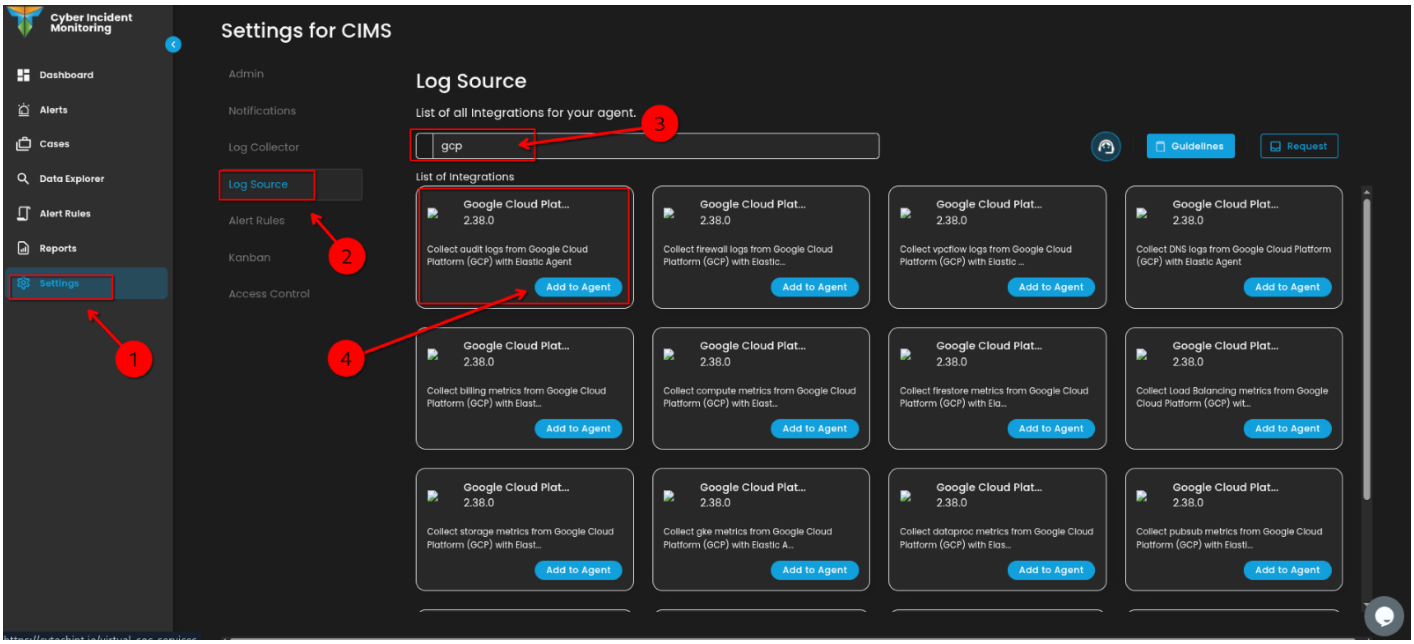
- **Project ID** - The Project ID is the Google Cloud project ID where your resources exist.
- **Credentials File** - Save the JSON file with the private key in a secure location of the file system, and make sure that the Log Collector Agent has at least read-only privileges to this file. Specify the file path in the Log Collector Agent integration UI in the "Credentials File" field. For example: /home/ubuntu/credentials.json.
- **Pub/Sub Topic** - Name of the topic where the logs are written to.
- **Subscription** - Use the short subscription name here, not the full-blown path with the project ID. You can find it as "Subscription ID" on the Google Cloud Console.

**After setting up GCP. Go to> CISO Workplace to integrate your log source. Please follow the instructions below:**

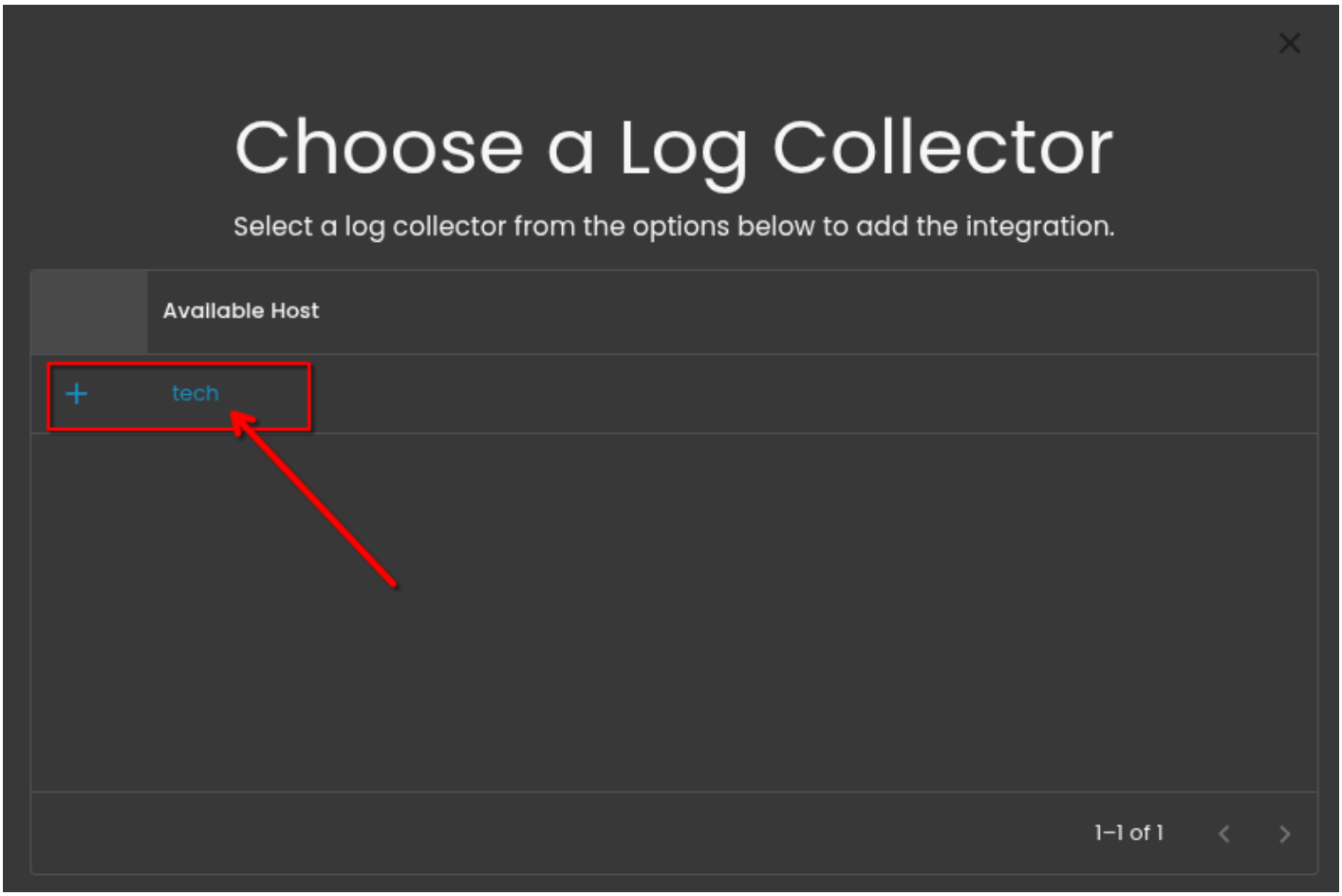
**Step1: Log in CISO Workplace>CISO Workplace Modules>Cyber Monitoring>Cyber Incident Management**



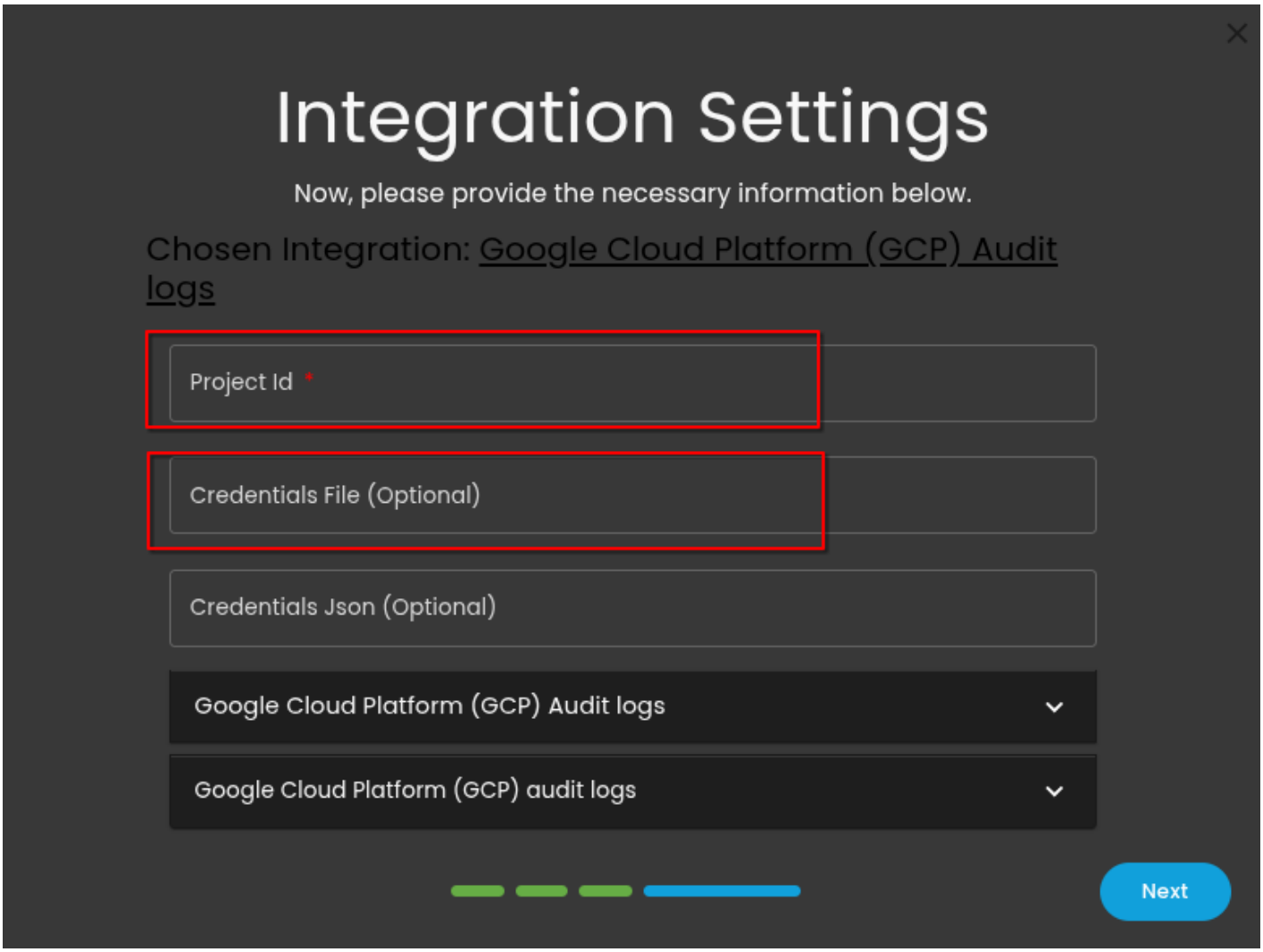

**Step2: Navigate through Settings>Log Source>Search Bar(type GCP)>Choose the type of GCP*(for example- Google Cloud Platform (GCP) Audit Logs - Collect audit logs from Google Cloud Platform (GCP) with Elastic Agent)*>Click "*Add to Agent*".**



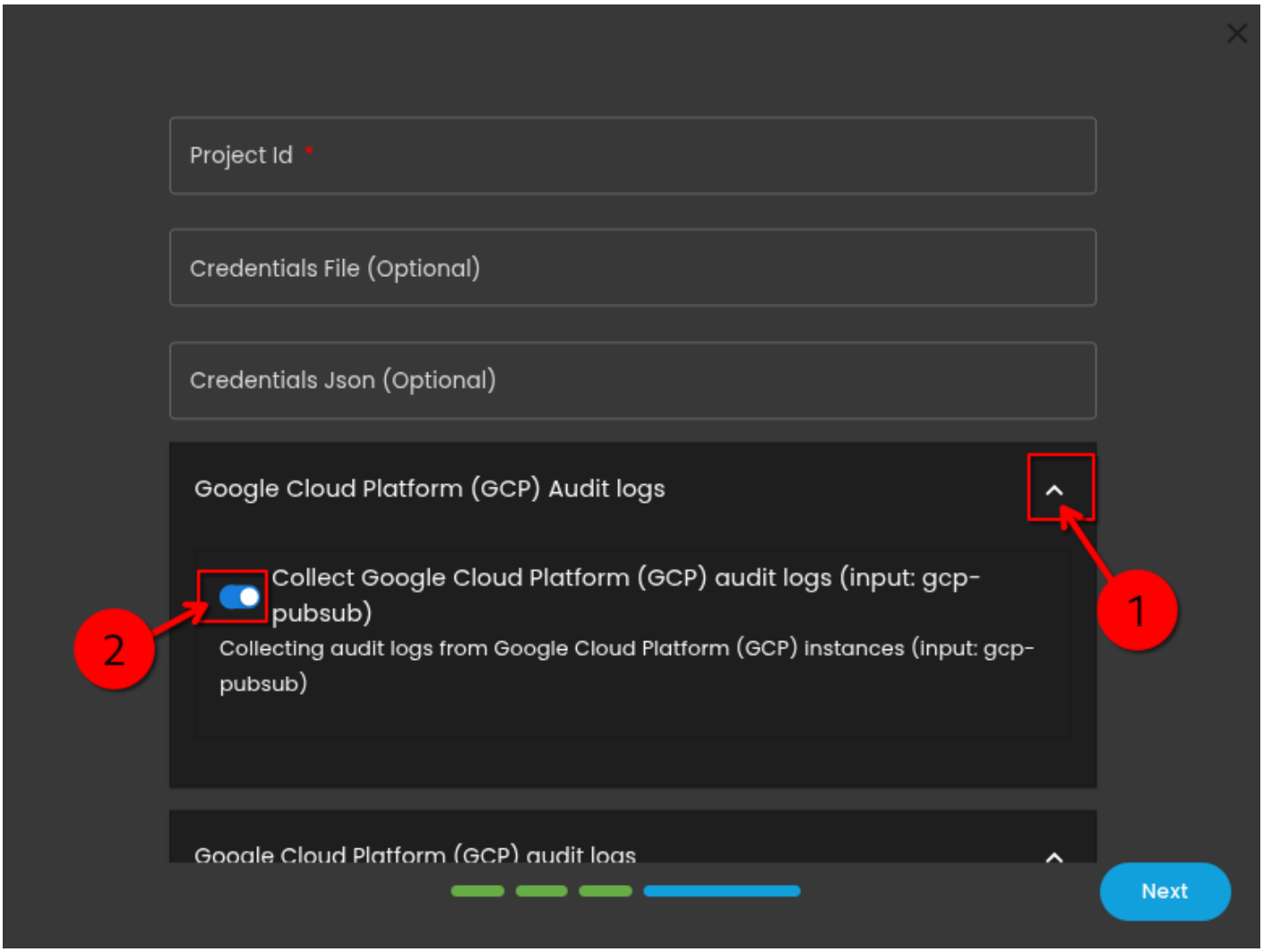

## Step3: Choose your "Log Collector".



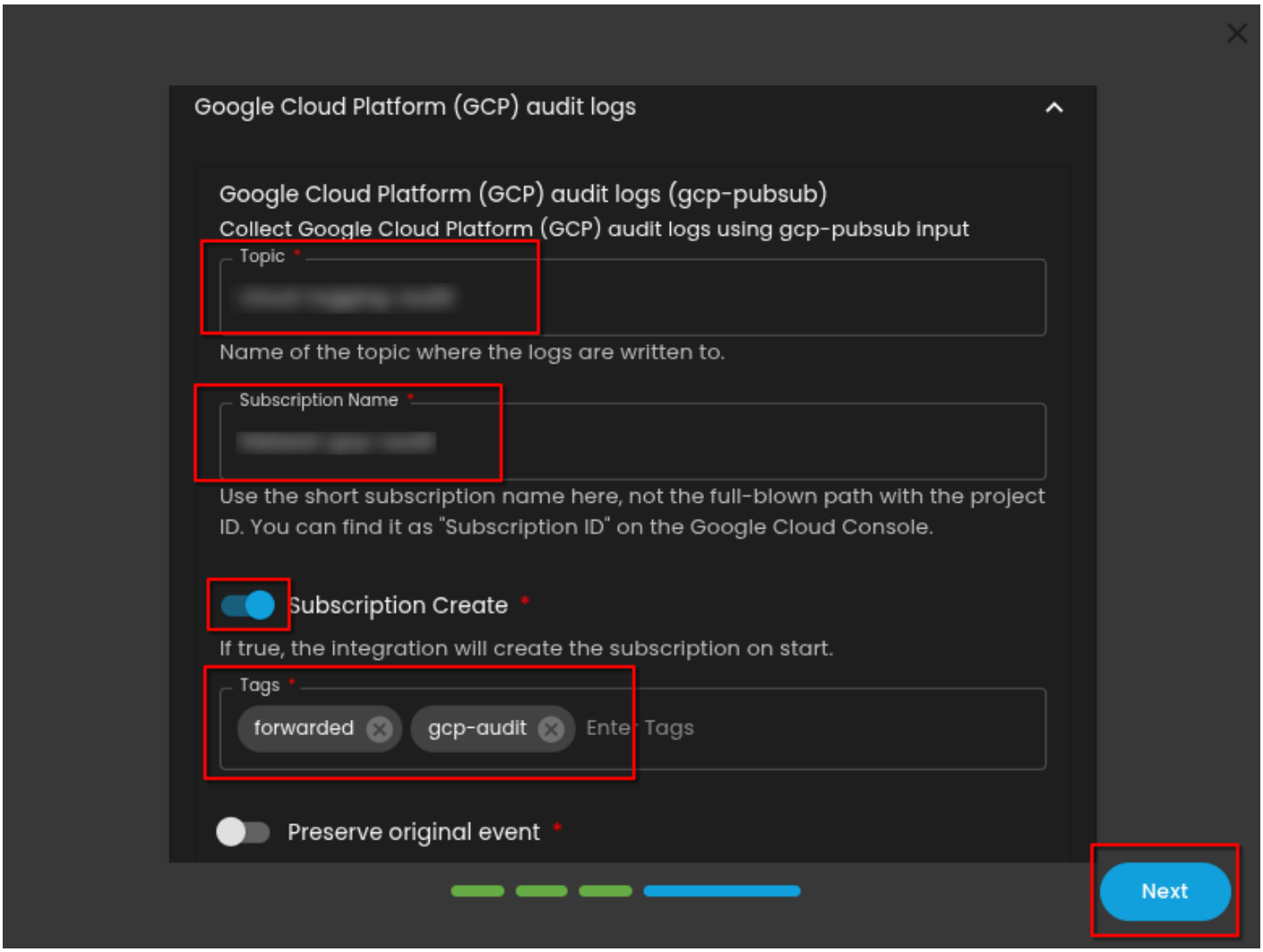

## Step4: Provide the "Project ID" and "Credentials File".



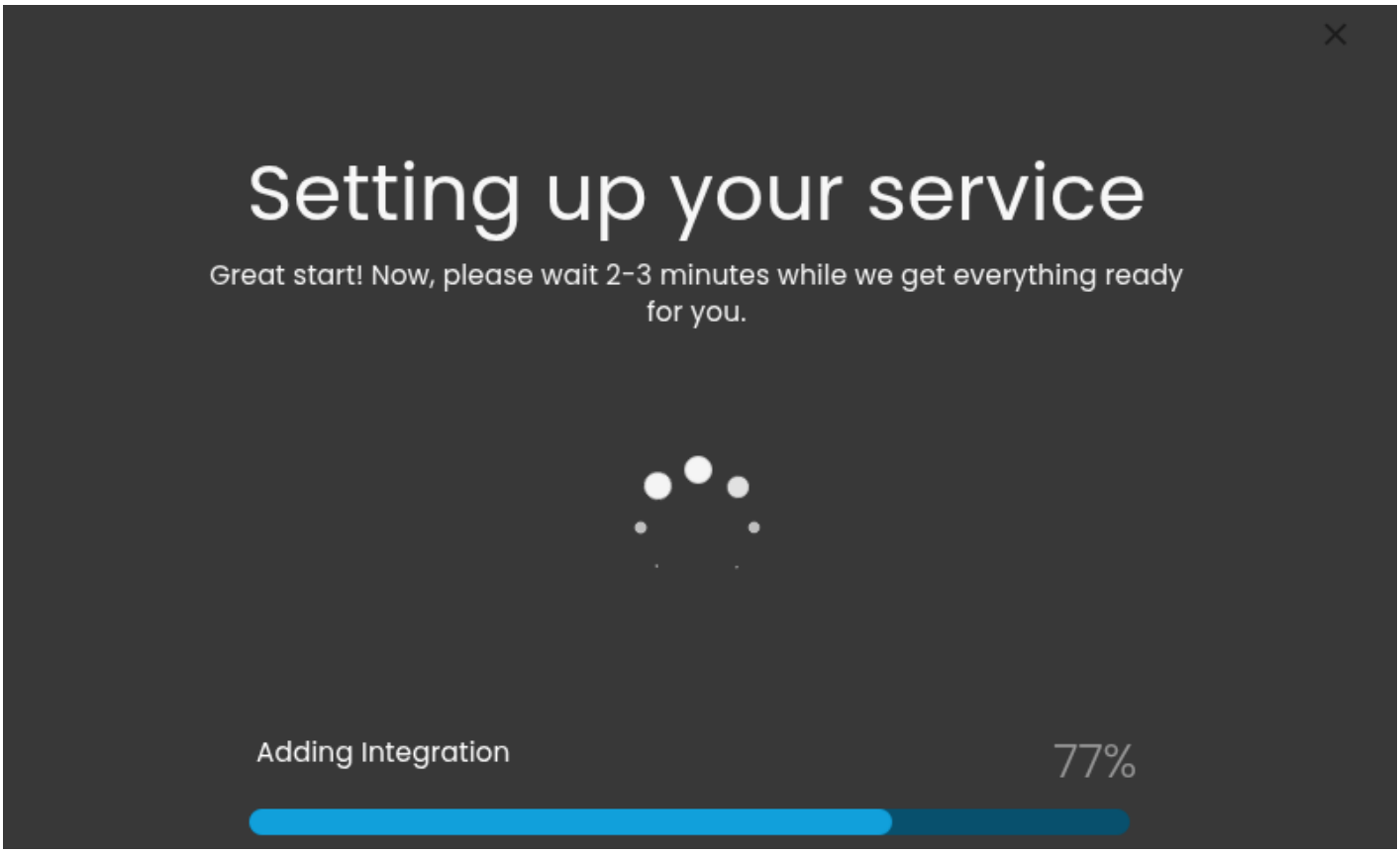

**Step5: Click down the arrow button and make sure to "enable" Collect Google Cloud Platform (GCP) audit logs.**



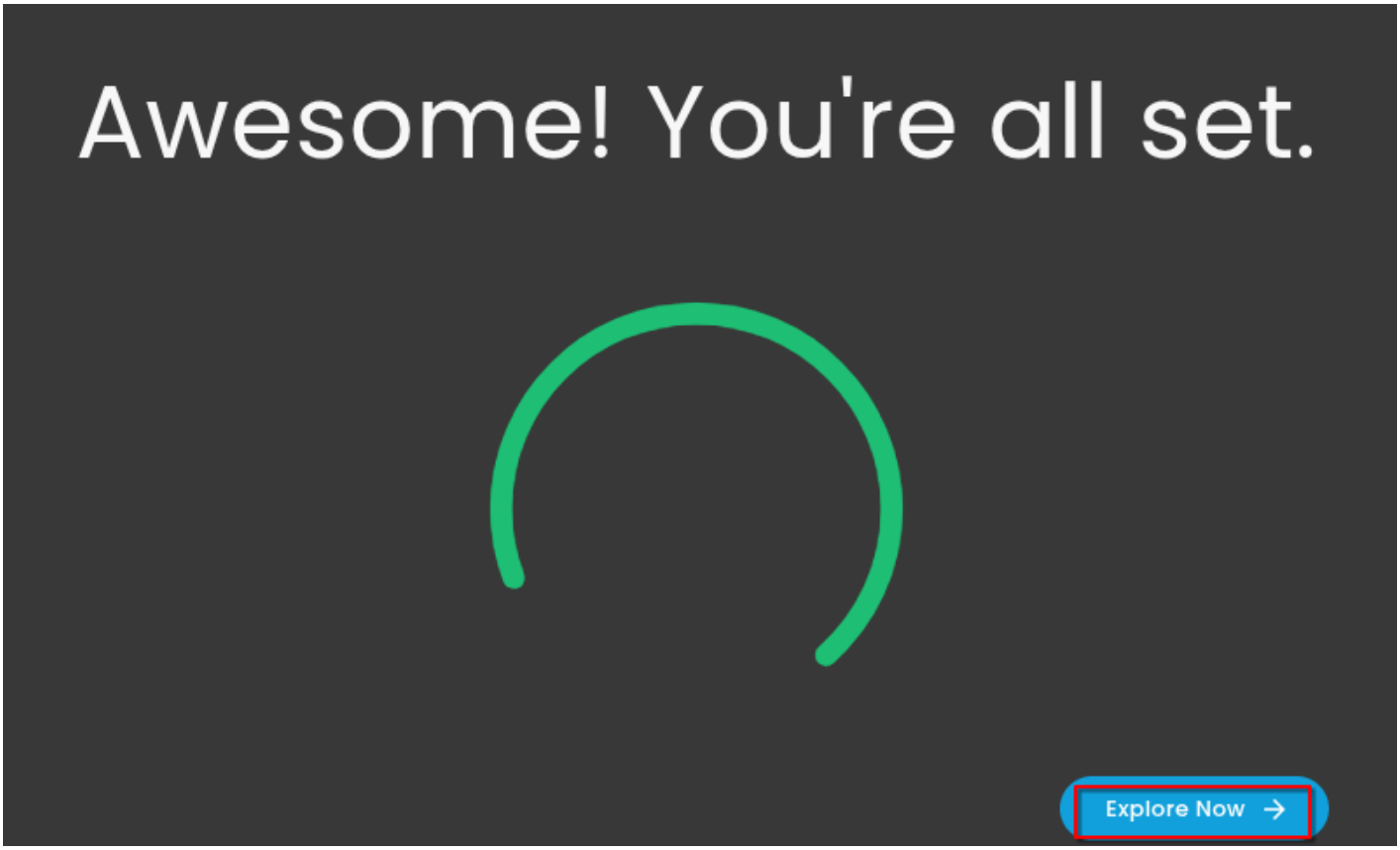

**Step6: In the Google Cloud Platform (GCP) Audit logs. Provide the "Topic" and "Subscription Name". Additionally, make sure to enable "Subscription Create" and enter "Tags"(*forwarded and gcp-audit*) by clicking the box. Click "Next" to proceed.**




**Step7: Wait for a couple of moment to finalize your integration.**




**Step8: A confirmation that the integration is finish installing.**



Documentation reference: *https://www.elastic.co/guide/en/integrations/current/gcp.html*

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

---

Revision #6
Created 14 April 2025 07:05:48 by Richmond Abella
Updated 30 April 2025 05:46:30 by Richmond Abella