NG SIEM - GCP CSPM Integration

The Google Cloud integration collects and parses **Google Cloud Audit Logs**, **VPC Flow Logs**, **Firewall Rules Logs,** and **Cloud DNS Logs** that have been exported from **Cloud Logging** to a **Google Pub/Subtopic sink** and collects **Google Cloud metrics** and metadata from **Google Cloud Monitoring.**

Logs

- **Firewall Logs:** Record allowed and denied network traffic based on firewall rules.
- **VPC Flow Logs:** Capture IP traffic flowing to and from network interfaces in a VPC.
- **DNS Logs:** Track DNS queries and responses handled by Google Cloud DNS.
- **Load Balancing Logs:** Provide request-level logs of traffic handled by load balancers, including latency and backend info.

Metrics

- **GCP Billing Metrics**: Track resource usage and cost across GCP services.
- **GCP Compute Metrics**: Monitor performance of Compute Engine instances (CPU, memory, disk, etc.).
- **GCP Firestore Metrics**: Provide insights into Firestore usage like reads, writes, and storage.
- **GCP Load Balancing Metrics**: Measure load balancer traffic, request counts, latency, and backend health.
- **GCP Storage Metrics**: Report usage, operation counts, and latency for Cloud Storage buckets.
- **GCP GKE Metrics**: Monitor Kubernetes clusters including node health, pod usage, and resource consumption.
- **GCP Dataproc Metrics**: Track job status, cluster usage, and Hadoop/Spark performance in Dataproc.
- **GCP PubSub Metrics**: Show message throughput, subscription rates, and processing latency.
- **GCP Redis Metrics**: Display memory usage, operations per second, and cache hit/miss rates for Memorystore Redis.
- **GCP Cloud Run Metrics**: Measure request counts, container instance metrics, and response times.
- **GCP CloudSQL Metrics**: Provide visibility into database performance, including connections, query latency, and CPU usage.

Authentication

To use the **Google Cloud Platform (GCP)** integration, the client must configure a **Service Account (SA)** that represents a non-human identity requiring access to **GCP** resources.

Service Account

First, you need to create a Service Account. A Service Account (SA) is a particular type of Google account intended to represent a non-human user who needs to access the GCP resources.

The AQUILA Agent uses the SA to access data on Google Cloud Platform using the Google APIs.

IAM Service Account Roles

For CSPM-GCP Integration

- **Browser:** Access to browse GCP resources.
- **Cloud Asset Viewer:** Read only access to cloud assets metadata

Logs Collection Configuration

The **Logs Collection Configuration** defines how log data is exported, transmitted, and processed within the system. It enables seamless integration between **Cloud Logging** and other Google Cloud services to ensure logs are efficiently collected, stored, and made available for analysis or monitoring.

Requirements

- **Pub/Sub Topic:** A **Pub/Sub topic** is a messaging channel that allows publishers to send messages asynchronously to multiple subscribers without them needing to know each other.
- **Subscription:** Subscriptions are named resources that receive messages on a particular topic. A subscriber client receives messages from a subscription and processes them.
- **Log Sink:** A log sink is a configuration that routes log entries from **Cloud Logging** to a chosen destination — such as **Cloud Storage**, **BigQuery**, or a **Pub/Sub topic** — for storage, analysis, or further processing.

> 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.

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"

Enable API Service

The client can enable their API through the **APIs & Services** section. To access it, click the ☰ **(navigation menu)** icon to open the **sidebar**, then hover over **APIs & Services** and select **Enabled APIs & Services**. Alternatively, the client can locate it using the **search bar** at the top of the page. Next, click **Library**, search for the required API services, and enable them.

- **Cloud Asset API:** Provides metadata inventory and history of GCP resources and IAM policies for security analysis, audit, and compliance.
- **Cloud SQL Admin API:** Enables programmatic management of Cloud SQL instances, including creation, configuration, and backups.
- **Memorystore for Redis API:** Allows automated management of Redis instances on Memorystore, including provisioning, scaling, and configuration.

Service Account Key

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).

> **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.

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

Revision #8
Created 23 September 2025 08:05:20 by Richmond Abella
Updated 3 December 2025 07:17:29