Work instruction:

**Google Security Command Centre Integration to Wazuh SIEM**

Prepared by Nasim Emadi

13/05/2023

Contents

[Generating GCP service account required for Publishing SCC findings 1](#_Toc134913020)

[Configuring Pub/Sub in GCP SCC project 5](#_Toc134913021)

[Create Topic 5](#_Toc134913022)

[Create Pub/Sub 7](#_Toc134913023)

[Create Sink (log Router) 10](#_Toc134913024)

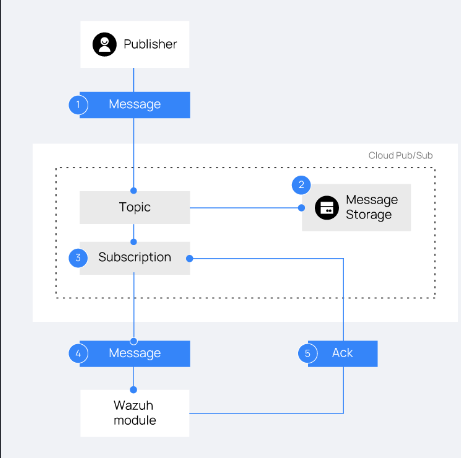
[Wazuh Configurations 13](#_Toc134913025)

[Installing pre-requisite applications for gcp-pubsub 13](#_Toc134913026)

[Adding Subscription to Wazuh config 14](#_Toc134913027)

[Sample of expected result 17](#_Toc134913028)

SCC to SIEM (Wazuh) integration data flow model



Ref: <https://documentation.wazuh.com/current/gcp/index.html>

This data flow reference diagram depicts how SCC (here as Publisher) findings gets exported to Topic and the Wazuh module as subscriber receives the findings in different project.

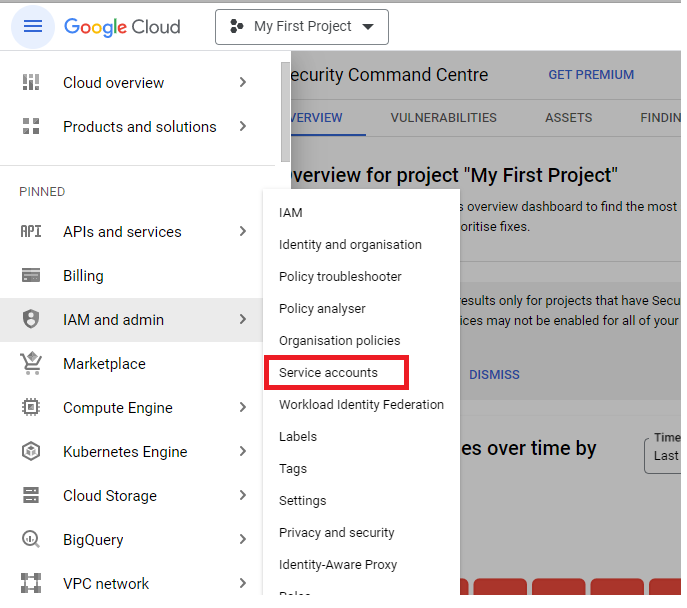
1. SCC Module as publisher application, creates a topic in the Cloud Pub/Sub service and sends messages to the topic.
2. Each published message (SCC findings) is retained until it is acknowledged by the Wazuh module consuming messages from that subscription.
3. The Wazuh module pulls the messages using its subscription to the Cloud Pub/Sub service.
4. The Wazuh module receives all messages from its subscription and acknowledges each one to the Cloud Pub/Sub service.
5. Finally, the messages are removed from the subscription’s message queue.

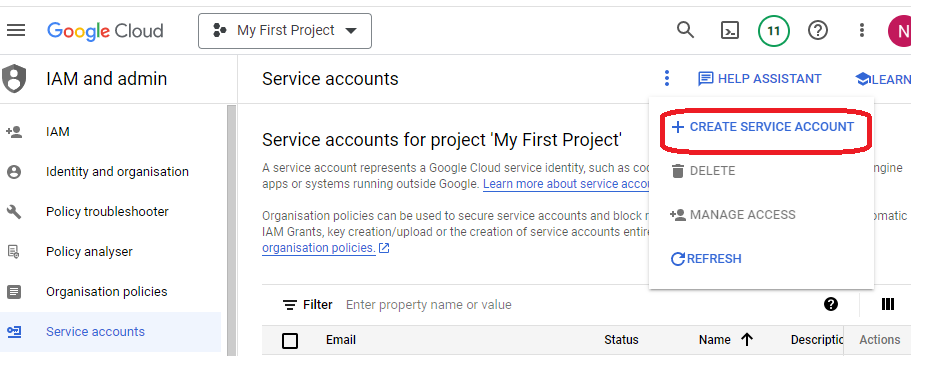
# Generating GCP service account required for Publishing SCC findings

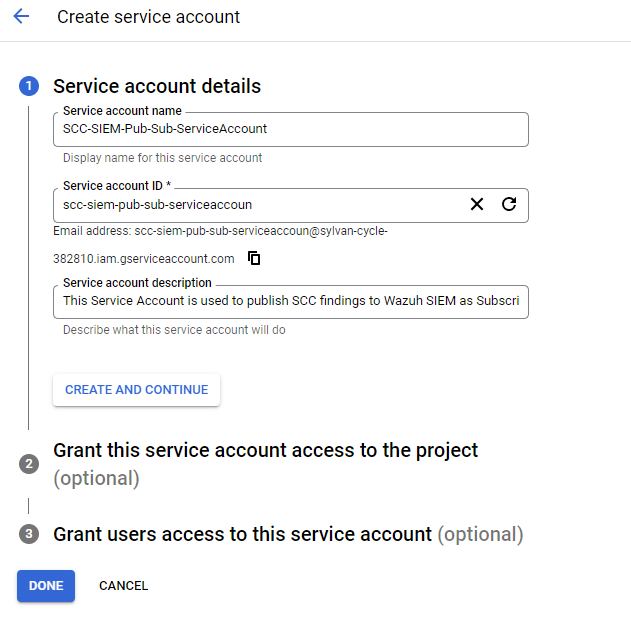
Ref: <https://documentation.wazuh.com/current/gcp/prerequisites/credentials.html>

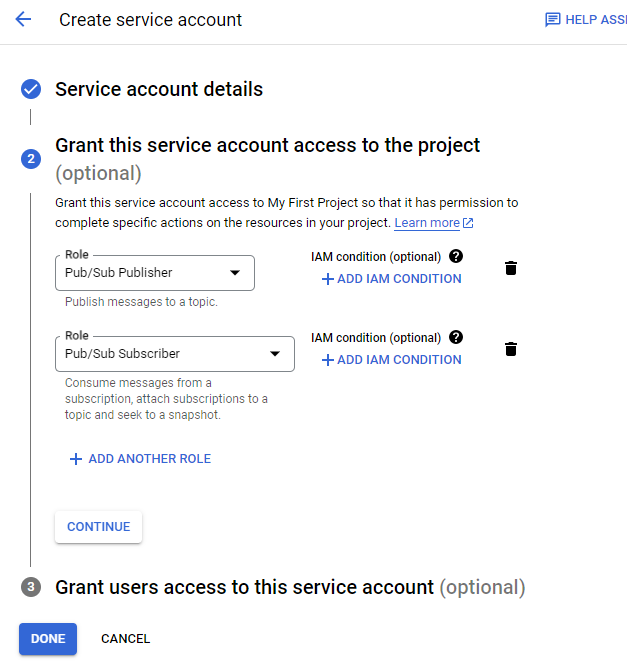
In order to make the Wazuh GCP module pull log data from Google Pub/Sub or Google Storage, it will be necessary to provide access credentials so that it can connect to them.

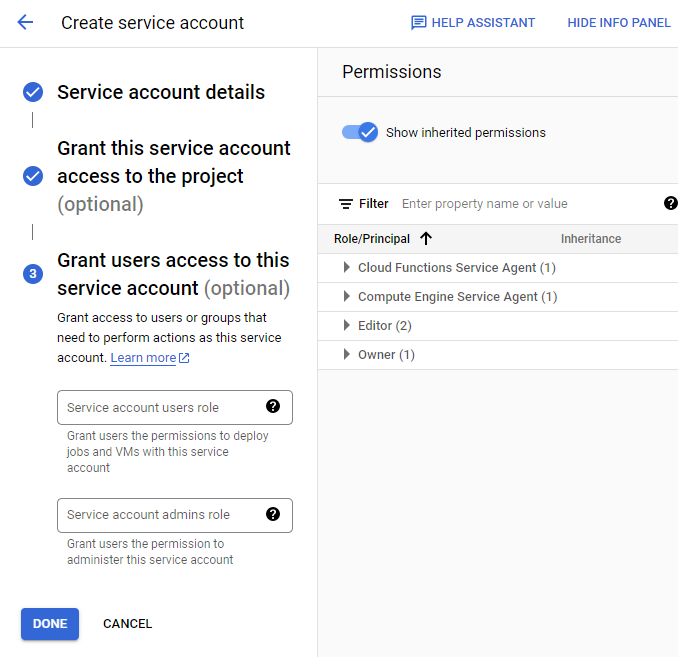
To do this, it is recommended to create a service account with the Pub/Sub or Storage permissions and then create a key. It is important to save this key as a JSON file as it will be used as the authentication method for the GCP module.

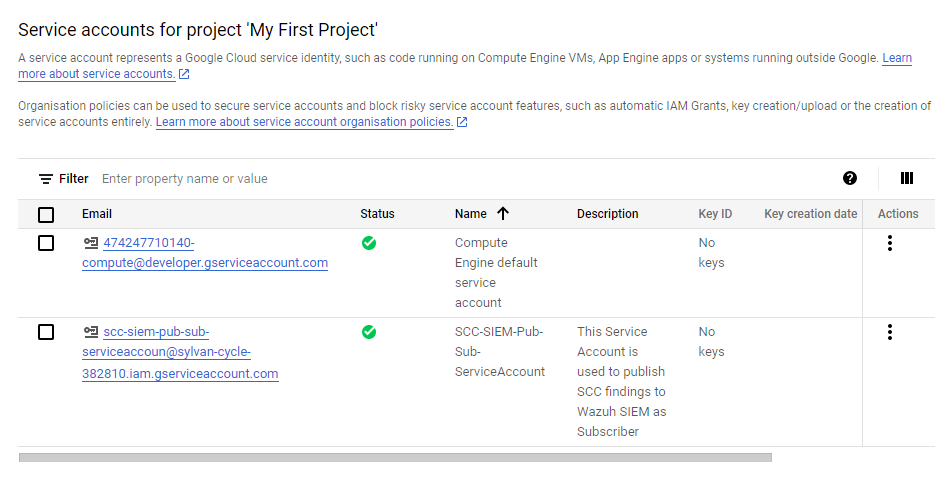




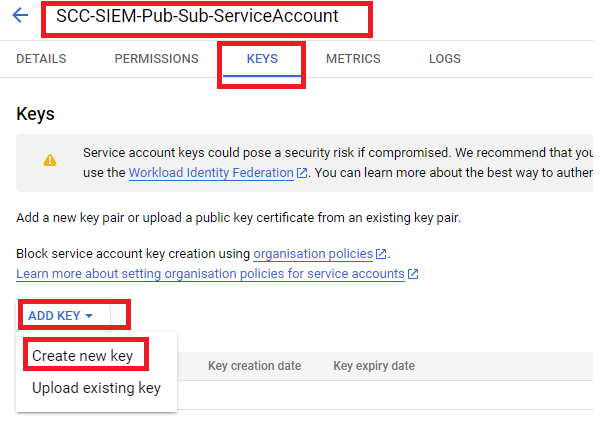








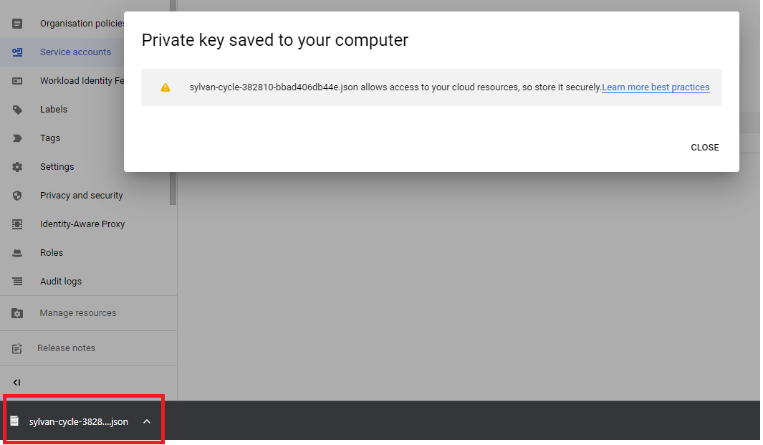
Create a private key for created service account.



A screenshot of a computer

Description automatically generated with medium confidence

Download the key file on your computer.



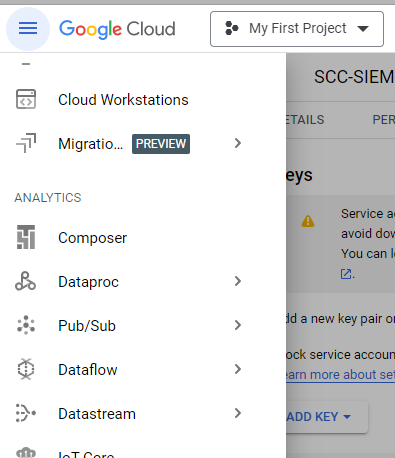
# Configuring Pub/Sub in GCP SCC project

Google Cloud Pub/Sub is a fully-managed real-time messaging service that allows you to send and receive messages between independent applications.

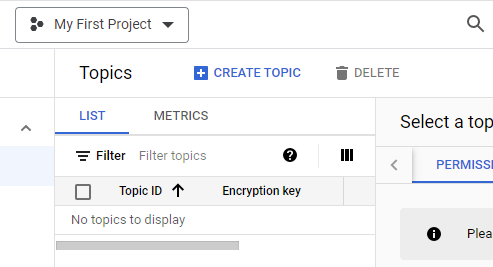
We use it to get security events from the Google Cloud Security Command Centre without creating a special logic to avoid reprocessing events.

## Create Topic

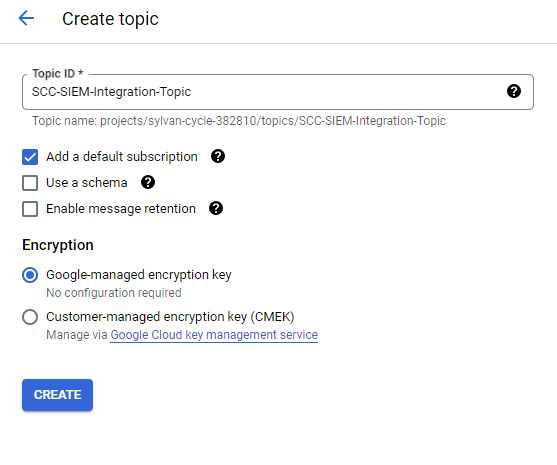
Open pub/sub from GCP console in SCC project.



Create topic:



Give the topic a name and create.



## Create Pub/Sub

In SCC project, open Security Command Centre(SCC), select findings tab and click on export, then select “Cloud Pub/Sub”.

A screenshot of a computer

Description automatically generated with medium confidence

Give it a name and description.

A screenshot of a computer

Description automatically generated with low confidence

Select current project (SCC and topic is created under that) as well as created topic in revious step.

A screenshot of a video

Description automatically generated with medium confidence

Add filter about which level of findings need to gets reported to SIEM.

A screenshot of a computer

Description automatically generated with medium confidence

Click save to have pub/sub object created.

A screenshot of a search engine

Description automatically generated with low confidence

A black rectangle with white text

Description automatically generated with medium confidence

## Create Sink (log Router)

In GCP console menu, Select “log router” under log.

A screenshot of a computer

Description automatically generated

Create Sink

A screenshot of a computer

Description automatically generated

A screenshot of a login form

Description automatically generated with low confidence

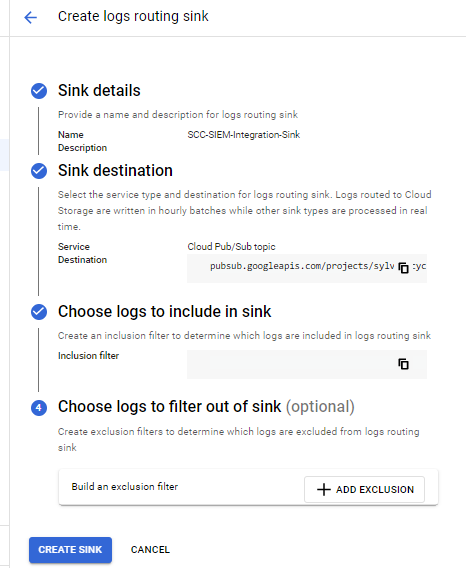
Select “Cloud Pub/Sub topic” for service type,

Then select created pub/sub topic in step1.

A screenshot of a computer

Description automatically generated with medium confidence

Click “Create Sink”



# Wazuh Configurations

## Installing pre-requisite applications for gcp-pubsub

Wazuh server has built-in google cloud integration modules, but it needs python3 and pip3 to be installed before activation. Here is how to install these prerequsitives as per Wazuh documentation.

Upon installing Wazuh server (Refer. to <https://documentation.wazuh.com/current/deployment-options/elastic-stack/all-in-one-deployment/index.html> for al-in-one server installation guide), run following commands to install prerequisite applications in Ubuntu (for other linux versions refer to Wazuh documentation (<https://documentation.wazuh.com/current/gcp/prerequisites/dependencies.html>)

# apt-get update && apt-get install python3

# apt-get update && apt-get install python3-pip

# pip3 install --upgrade pip

# pip3 install cachetools==4.1.0 certifi==2022.12.07 cffi==1.14.4 chardet==3.0.4 charset-normalizer==2.0.4 google-api-core==1.30.0 google-auth==1.28.0 google-cloud-core==1.7.1 google-cloud-pubsub==2.7.1 google-cloud-storage==1.39.0 google-crc32c==1.1.2 google-resumable-media==1.3.1 googleapis-common-protos==1.51.0 grpc-google-iam-v1==0.12.3 grpcio==1.38.1 idna==2.9 libcst==0.3.20 mypy-extensions==0.4.3 packaging==20.9 proto-plus==1.19.0 protobuf==3.19.6 pyasn1-modules==0.2.8 pyasn1==0.4.8 pycparser==2.20 pyparsing==2.4.7 pytz==2020.1 PyYAML==5.4.1 requests==2.25.1 rsa==4.7.2 setuptools==59.6.0 six==1.14.0 typing-extensions==3.10.0.2 typing-inspect==0.7.1 urllib3==1.26.5

A screenshot of a computer

Description automatically generated

## Adding Subscription to Wazuh config

Ref: <https://documentation.wazuh.com/current/user-manual/reference/ossec-conf/index.html>

The ossec.conf file is the main configuration file on the Wazuh manager, and it also plays an important role on the agents. It is located at /var/ossec/etc/ossec.conf both in the manager and agent on Linux machines. On Windows agents, we can find it at C:\Program Files (x86)\ossec-agent\ossec.conf. It is recommended to back up this file before making changes to it. A configuration error may prevent Wazuh services from starting up.

Wazuh makes use of the gcp-bucket module. the authentication file is always specified in the ossec.conf configuration file using the <credentials\_file> tag.

Upload GCP service account credential file(.jsoon) created earlier, to Wazuh manager .

Backup file /var/ossec/etc/ossec.conf on Wazuh manager:

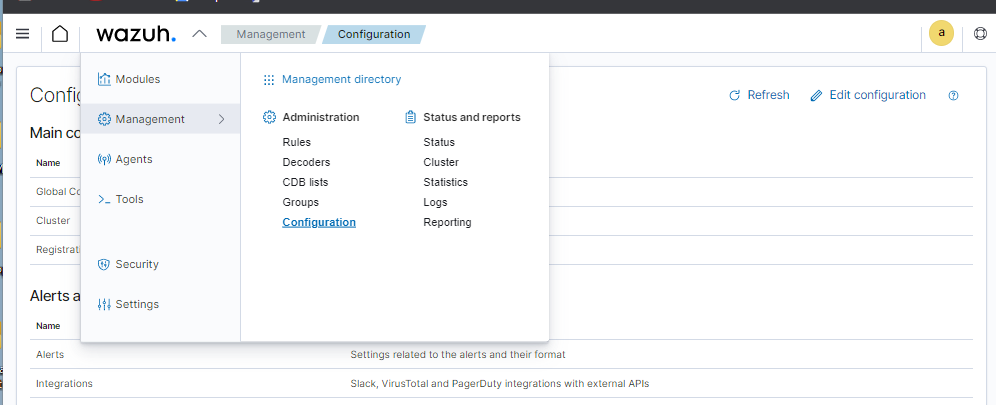
#cp -p /var/ossec/etc/ossec.conf /var/ossec/etc/ossec.conf.bkp

Move credential file to folder /etc and rename it as “credentials.json”

Confirm file exists:

# ls -ltr /etc/credentials.json

Edit configuration file in Wazuh server portal (Management -> Configurations -> Edit Configuration button”



Here there should be a block of XML definitions to define google cloud pub sub module.

Following tags can be defined here (all of them are not necessary though):

* project\_id: String. Google Cloud Project ID (name, not number). Required.
* subscription\_name: String. Name of the subscription to read from. Required.
* credentials\_file: String. The path to the Google Cloud credentials file. JWT Tokens. It must allow both relative (to $HOME\_INSTALLATION) and absolute paths. Required.
* interval: String. The amount of time between each pull. Default: 1h. (It must allow the format: 1h, 1d, 20m, 1405s).
* max\_messages: Integer. The number of maximum messages pulled in each iteration. Default: 100.
* enabled: String. Enable or disabled the module. Values: yes/no.
* pull\_on\_start: String. Trigger the pulling in case of an agent start or restart. Values: yes/no. Default: yes.

Here is required block for SCC integration:

<gcp-pubsub>

<pull\_on\_start>yes</pull\_on\_start>

<interval>1m</interval>

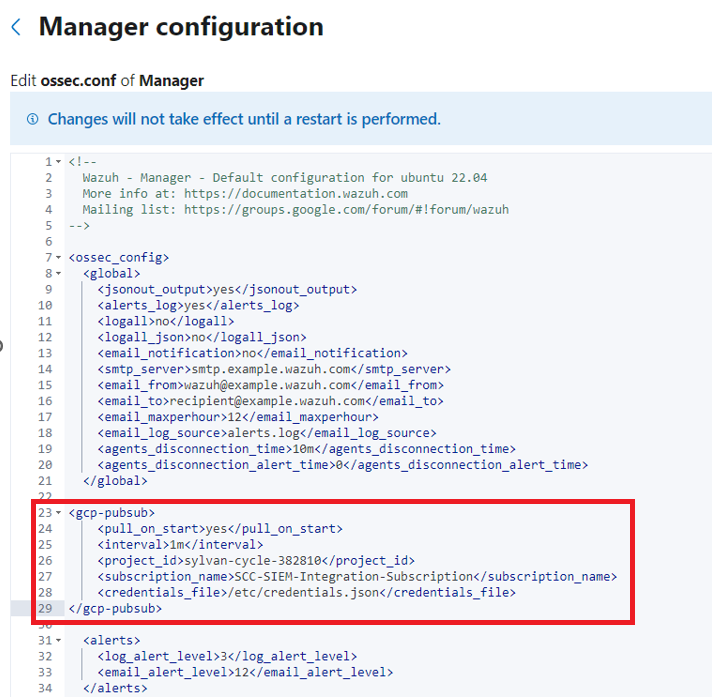
<project\_id>sit-23t1-vulnerability-2c59c04</project\_id>

<subscription\_name>SCC-SIEM-Integration-Topic-sub</subscription\_name>

<credentials\_file>/etc/credentials.json</credentials\_file>

</gcp-pubsub>

Locate the above block under “global” XML tag as you see below:

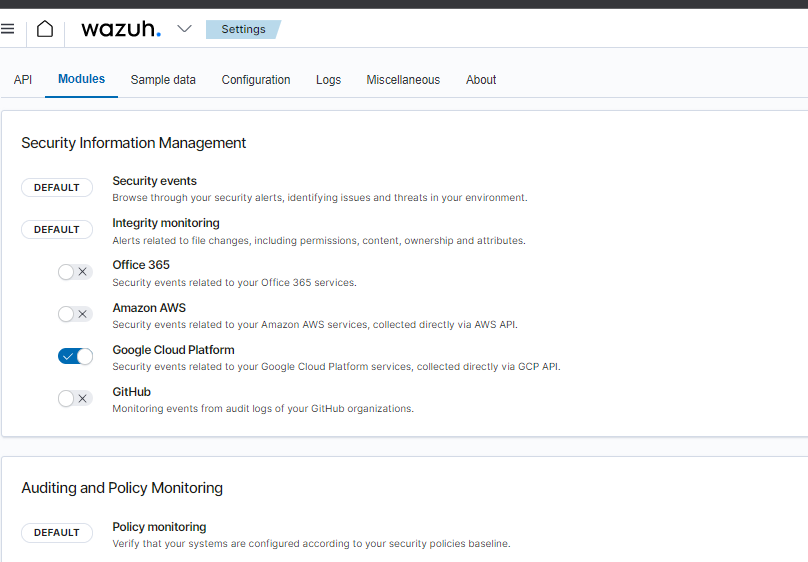


Save and Click on “Restart Manager” button to apply the changes.

Confirm setting from Management -> Configuration, Google Cloud Pub/Sub.

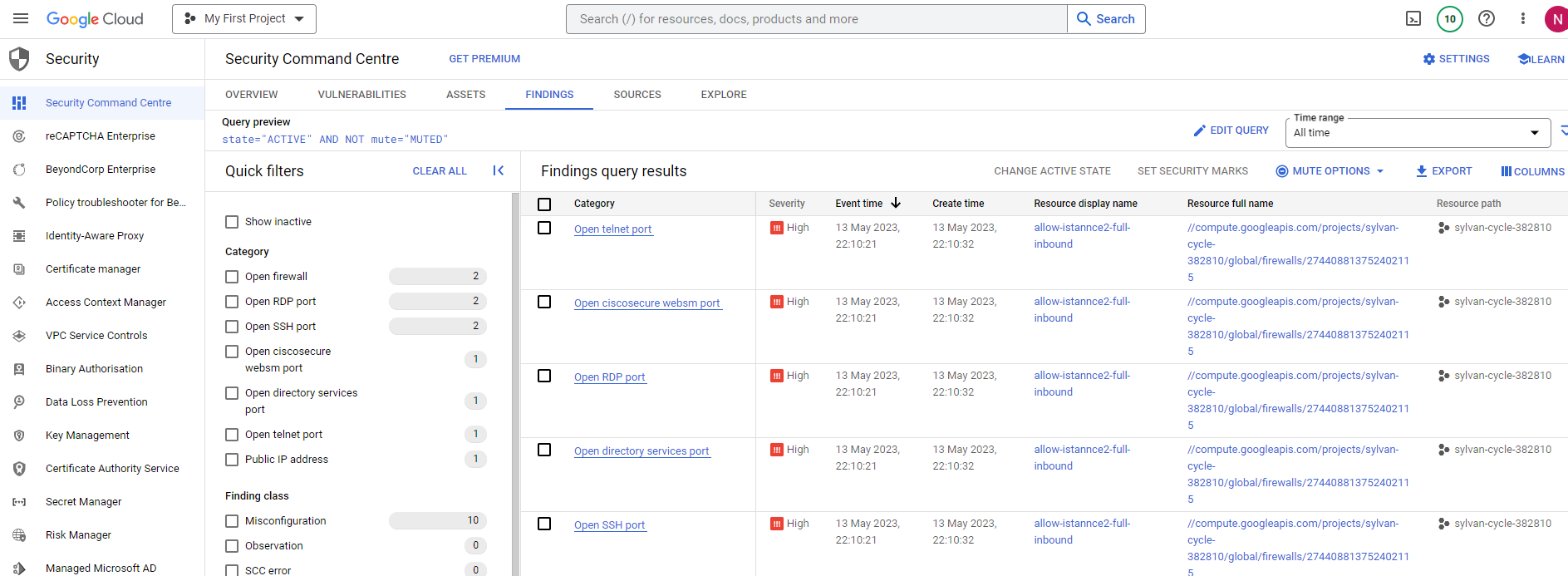
A screenshot of a computer

Description automatically generated



# Sample of expected result

First project SCC found an issue on firewall rules.



Second project with Wazuh instance

A screenshot of a computer

Description automatically generated with medium confidence

We have same findings reported to Wazuh

A screenshot of a computer

Description automatically generated with medium confidence