Google Cloud Security Command Center Integration

Last Revised: April 24, 2019

Table of Contents

Google Cloud Security Command Center

The Google Cloud Security Command Center (CSCC) tool is designed to:

1. Obtain Tenable.io asset and vulnerability data.
2. Convert the obtained Tenable data to the Google Cloud Security Command Center format.
3. Upload the converted data to the Google Cloud Security Command Center.

You can run the Google Cloud Security Command Center tool as a docker image or command-line tool.

- To run the tool as a docker image, build the image and provide the required authorization to access the container.
- To run the tool as a command-line tool, install the required python modules and run the tool using environment variables or by passing the required run-time parameters.

Requirements

- Tenable.io administrator account
- API Keys for use with the Exports API with Tenable.io
- Google Cloud service account with required permissions to edit Security Center Findings Editor, and Security Center Findings State Setter roles
- A host that can run a Python 3.x environment to act as a bridge for cloud-to-cloud communication

Installation

Run the following script to install the Google Cloud Security Command Center tool.

```
pip install tenable-cscc
```

Setup

To setup your Google Cloud Service account:

1. From the Google Marketplace, add the Tenable.io CSCC Service.
2. Copy the system generated source ID.

   Note: Be sure to save the source ID for later use.

3. Create a service key for the account you created using the steps in the create a service key section.
4. Create a new VM instance. This VM (Debian 9) stores the integration.
5. Type the following command to download the installation script.

   ```
   curl -o installer.sh https://raw.-
   githubusercontent.com/tenable/integration-cscc/master/install-tenable-
   cscc.sh
   ```

6. Type the following command to run the installer.

   ```
   chmod 755 installer.sh && sudo ./installer.sh
   ```

7. Copy the service key onto the host. For example, run: `/etc/google-account.json`
8. Update the variables in the `/etc/tenable-cscc.conf` file.
9. Type the following command to start the service.

   ```
   sudo systemctl start tenable-cscc
   ```

Options

Use the following command-line arguments and equivalent environment variables to configure Google Cloud Security Command Center.

```
Usage: tenable-cscc [OPTIONS]
Tenable.io -> Google Cloud Security Command Center Bridge
Options:
--tio-access-key TEXT           Tenable.io Access Key
--tio-secret-key TEXT           Tenable.io Secret Key
-b, --batch-size INTEGER        Export/Import Batch Sizing
-v, --verbose                   Logging Verbosity
-s, --observed-since INTEGER    The unix timestamp of the age threshold
-r, --run-every INTEGER         How many hours between recurring imports
-t, --threads INTEGER           How many concurrent threads to run for the
import.
-s, --service-account-file PATH
-i, --service-id TEXT           The GCP CSCC Source ID
--help                          Show this message and exit.
```

Usage

To run the import once, in the command line type the following.

```
tenable-cscc                                \
--tio-access-key {TIO_ACCESS_KEY}           \
--tio-secret-key {TIO_SECRET_KEY}           \
--service-account-file {SA_JSON_FILENAME}   \
--org-id {ORG_ID}
```

To run the import every hour, in the command line type the following.

```
tenable-cscc                                \
--tio-access-key {TIO_ACCESS_KEY}           \
--tio-secret-key {TIO_SECRET_KEY}           \
--service-account-file {SA_JSON_FILENAME}   \
--org-id {ORG_ID}
--run-every 1
```

Changelog

View the changelog.