GCP Cloud Security Engineer Exam Crash Course Lab 2

Data Loss Prevention

Create a DLP Test (Create Template, Job and Text file to load)

Cloud DLP Provides the ability to detect sensitive data within streams of data, structured text, files in storage repositories such as Cloud Storage and BigQuery, and even within images. (Helps you understand and manage your sensitive data)

Log in to your Google Cloud Platform Account

- Determine the project you will be creating credentials in.
- Search for Data Loss Prevention in the Search Console (Top of Console)
- You should arrive under Security and the DLP (Figure 1)

Figure 1 – Data Loss Prevention Console

Short Data Loss Prevention Exercise Lab
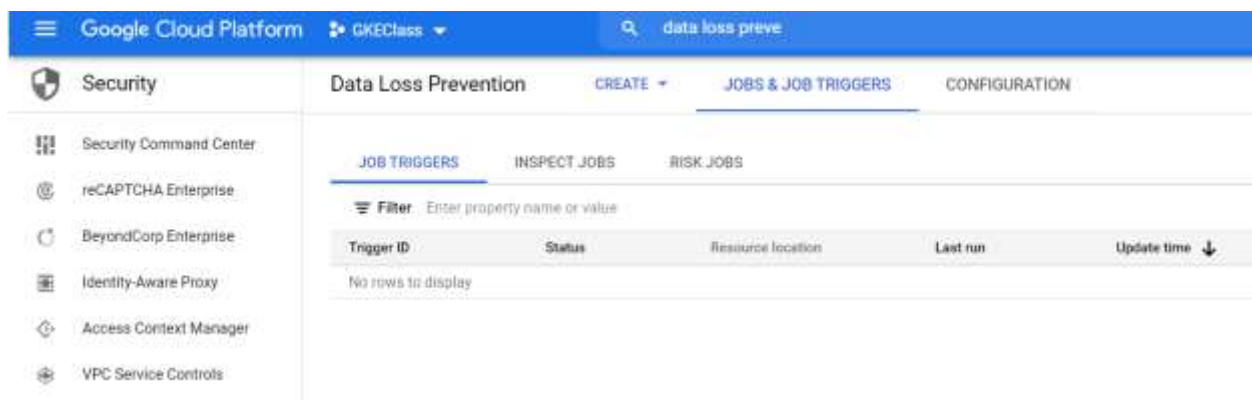
DLP can find PII data for example such as SSNs, Passport IDs, Addresses, Phones, etc. We want to create a template to scan for Social Security Numbers.

As show in Figure 2 Select "Create" and then Select "Template"

Figure 2 – Template Selection
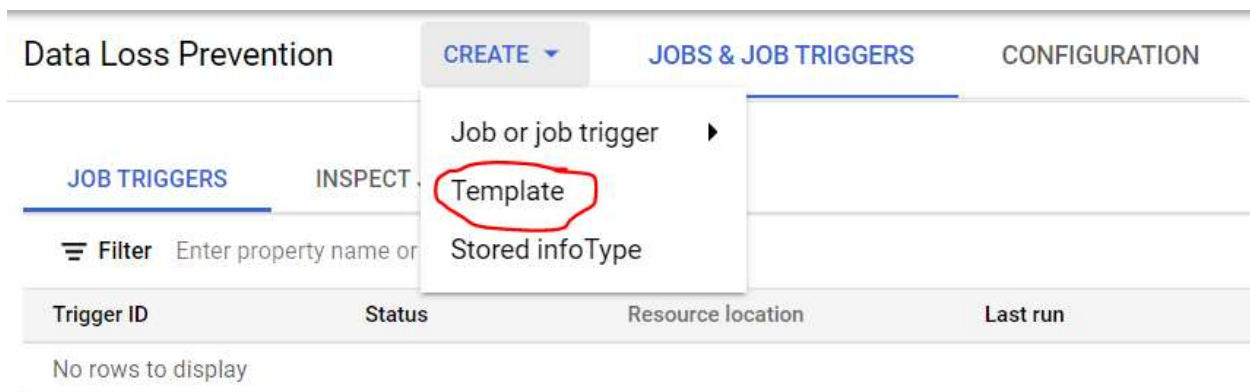
Now let's name the template enter information as in Figure 3

Once you complete entering the information Click "Continue"

Figure 3 – Create Template

← Create template

1 Define template

Template type *

Inspect (find sensitive data) ▼

Template ID

FindSSNNumbersProductionJulyVersion1

Letters, numbers, hyphens, and underscores allowed.   36 / 100

Display name

SSN Search July Cloud Storage

29 / 256

Description

Find SSN Numbers in Cloud Storage

33 / 256

Resource location *

South Carolina (us-east1) ▼ ❓

Resource preview: projects/gkeclass1/locations/us-east1/inspectTemplates/FindSSNNumbersProductionJulyVersion1
This cannot be changed

CONTINUE

2 Configure detection

CREATE   CANCEL

After clicking Continue we now go to Configure detection.   (This will let us configure what to search for and where)

Figure 4. Configure Detection

Short Data Loss Prevention Exercise Lab

After Selecting "Manage InfoTypes" as in above figure we now want to search in the Filter bar for "Social Security Number" (Select the Capitalized One) as in Figure 5 below. We also need to select the checkbox next to Name and then proceed to next menu by selecting "Done".

Figure 5 – Configure InfoTypes

Short Data Loss Prevention Exercise Lab

Figure 6 – Leave Defaults before creating.

Short Data Loss Prevention Exercise Lab

← Create template

✓ **Define template**

② **Configure detection**

InfoTypes   MANAGE INFOTYPES

ID ↑
US_SOCIAL_SECURITY_NUMBER

The sensitive data you want to scan for.

Inspection rulesets

Adds hotword and exclusion rules to further extend built-in and custom infoType detectors with powerful context rules. Learn more

[+ ADD A RULESET]

Confidence threshold

The likelihood that a scan finding matches a given infoType, bucketed into 5 categories from very unlikely to very likely. All findings lower than the threshold specified here will not be included in results. Learn more

Likelihood
Unspecified (use API default) ▼

*How you want the findings classified in the job details report.*

CREATE   CANCEL

Short Data Loss Prevention Exercise Lab

After selecting "Create"

Figure 7 – Inspection Template Details.

We have now created a template. We now need to scan for SSN number by configuring a Template so proceed back to the main DLP Menu as in Figure 8.

Figure 8 – Main DLP Menu with highlighted inspection selection path
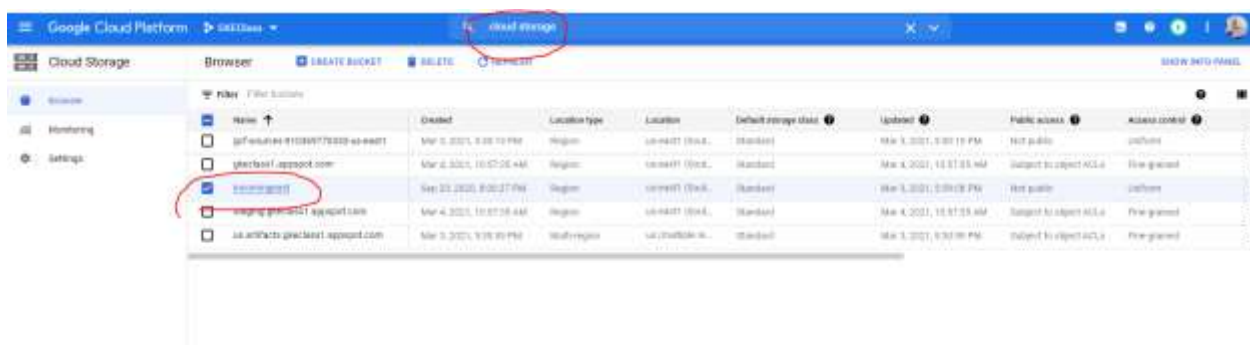
Short Data Loss Prevention Exercise Lab
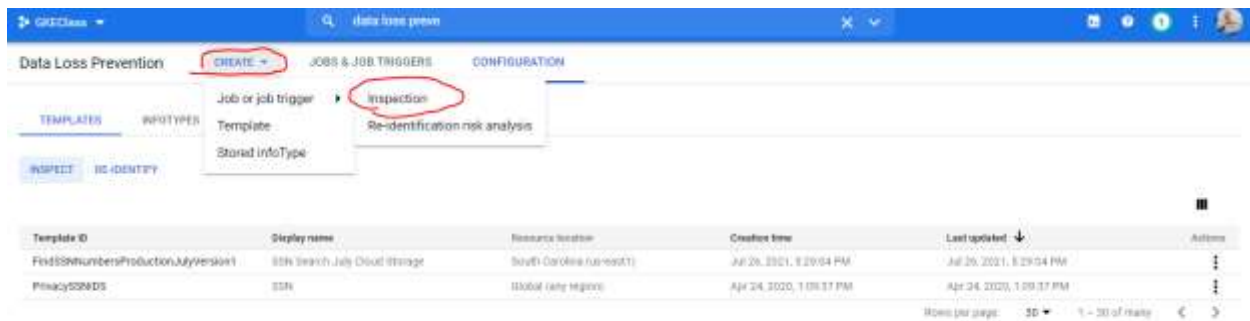
After selecting "Inspection" we know need to ensure we have a Cloud Storage Bucket and Objects to scan.

Proceed to Cloud Storage and select a bucket you may have (Pay attention to the Region you selected in the Template to match them up if you don't select Global in your template)

Below is the Cloud Storage Dashboard. I have highlighted the bucket I will use in Charleston. (You can use a bucket you already have or create a new one)

Figure 9 – Cloud Storage

(We will upload a text file to Cloud Storage called SSNTEST.

Figure 10 – SSN Test File Uploaded.

Short Data Loss Prevention Exercise Lab

Now let's go back to the DLP Dashboard and create a Job to scan.

Select Create

Figure 11 – DLP Configuration

After we select Create, we should select Job or Job Trigger > Inspection

Short Data Loss Prevention Exercise Lab

Figure 12 – Back to DLP Inspection

Enter Select Information as below in Figure 13.

Figure 13- Select Bucket and Location info.

Short Data Loss Prevention Exercise Lab

← Create job or job trigger

1 Choose input data

Name

Job ID
dlpscanssn1

Letters, numbers, hyphens, and underscores allowed.   11 / 100

Resource location *
South Carolina (us-east1)   ▼   ❓

Resource preview: projects/gkeclass1/locations/us-east1/dlpJobs/dlpscanssn1
This cannot be changed

Location

Specify the location of data stored in a Cloud Storage Bucket or BigQuery table.

Storage type *
Google Cloud Storage   ▼

Location type
Scan a bucket with optional include/exclude rules   ▼

Bucket name *
📁 incomingeast   BROWSE

Next scroll down and Select "Continue before Continue Detection (not shown here)

We now want point Configure Detection to the Template we created in the first steps. Below I selected the Template Name

Short Data Loss Prevention Exercise Lab

Figure 14- Select Template.

Short Data Loss Prevention Exercise Lab

← Create job or job trigger

✓ **Choose input data**

② **Configure detection**

Template

Templates are an optional way to use a single source for job configuration information. Learn more

Template name
projects/gkeclass1/locations/us-east1/inspectTemplates/FindSSNNumbersPr

∨ SHOW TEMPLATE DETAILS

InfoTypes   **MANAGE INFOTYPES**

ID ↑
CREDIT_CARD_NUMBER
EMAIL_ADDRESS
GCP_CREDENTIALS
IMEI_HARDWARE_ID
IP_ADDRESS
MAC_ADDRESS
MAC_ADDRESS_LOCAL
PASSPORT
PHONE_NUMBER
US_BANK_ROUTING_MICR

Rows per page: 10 ▼   1 – 10 of 14 ⟨ ⟩

Short Data Loss Prevention Exercise Lab
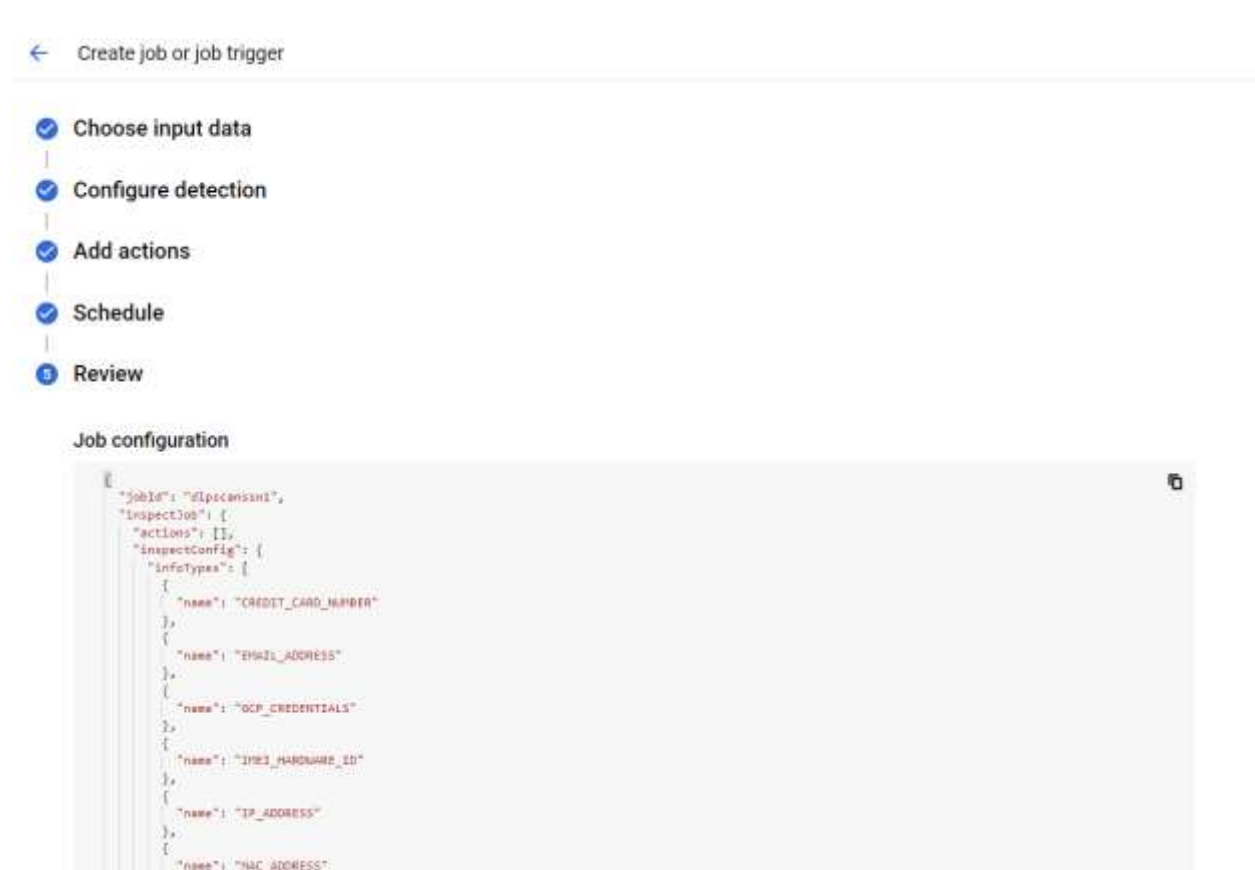
For the purpose of this demo the defaults for Steps 3-5 will suffice but certainly checkout the capabilities if you like.

Notice the configuration below.

Figure 15- Review

When you're ready select "Create" at the bottom of the Job Menu (Not shown here)

Below is a prompt that you will receive to confirm you ready to proceed.

Figure 15- Confirm Create

Short Data Loss Prevention Exercise Lab

Confirm job or job trigger create

It's possible for costs to grow rapidly, depending on the quantity of information Cloud DLP has to scan. Turn on sampling in configure detection, or see Keeping Cloud DLP costs under control to learn more.

CANCEL   CONFIRM CREATE

The creation will complete and will bring to the Job Menu. After about 2 or so the job should come back with a similar result in Figure 16 below

Figure 16 – Scan Results – Found an SSN/TIN Match.
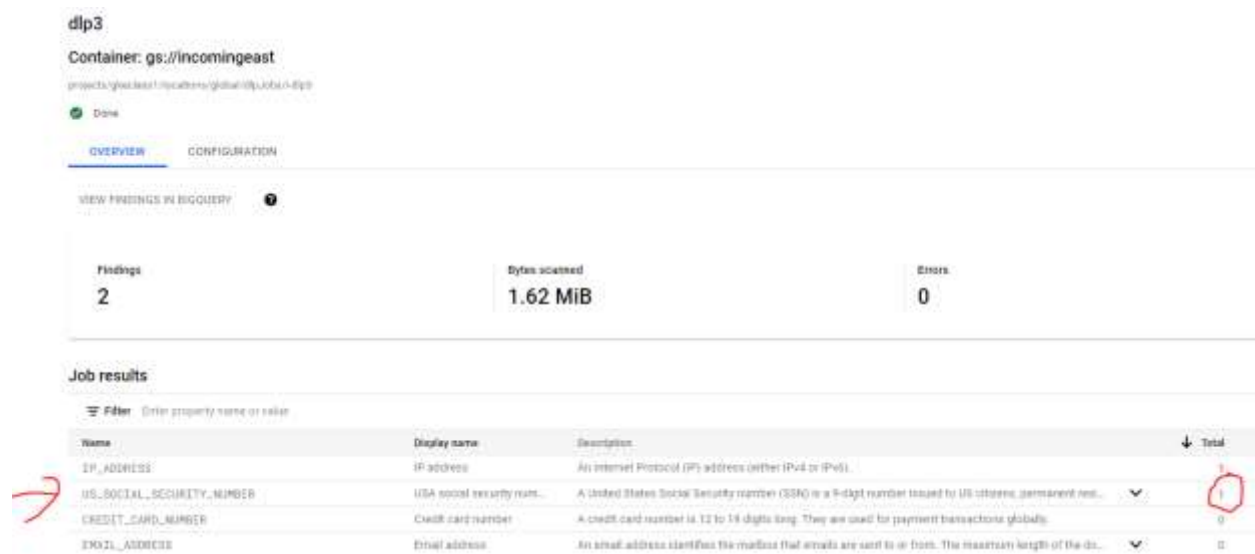
Note that when configuring these DLP jobs for a production environment we would really want to think out and plan our deployment. A simple job like would like to come up a lot of false positives.

End.

Short Data Loss Prevention Exercise Lab