

GCP Cloud Security Engineer Exam Crash Course Lab 2

Data Loss Prevention

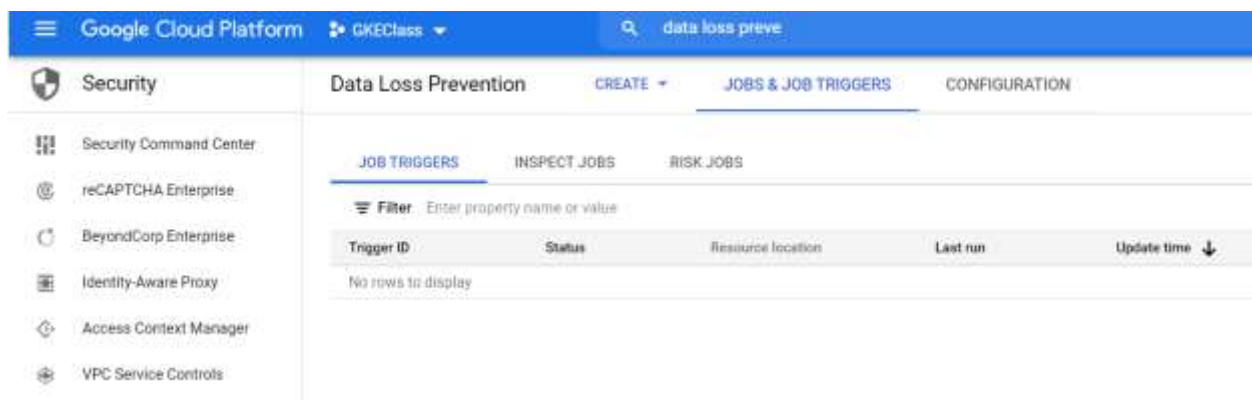
Create a DLP Test (Create Template, Job and Text file to load)

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)

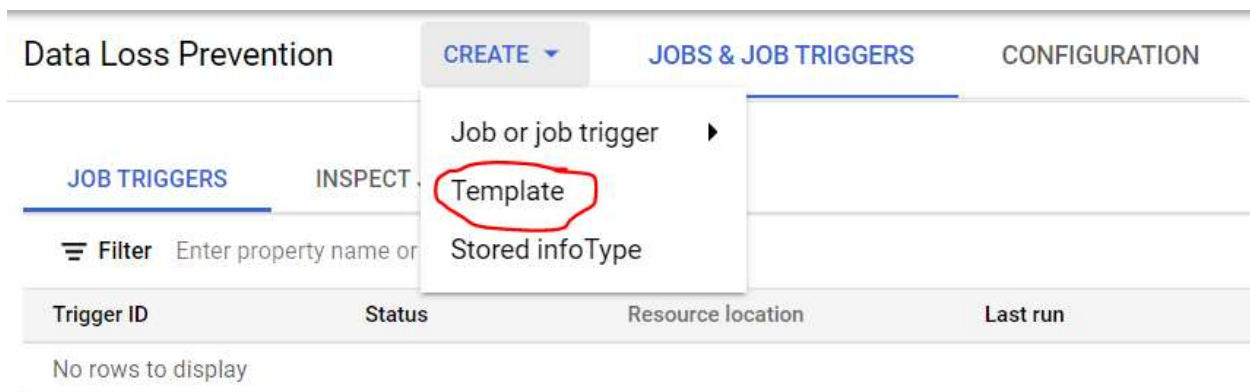
Figure 1 – Data Loss Prevention Console



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

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

[←](#) Create template

✓ Define template

2 Configure detection

InfoTypes

MANAGE INFOTYPES

ID	↑
No infoTypes selected	

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

Very likely

▼

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

CREATE

CANCEL

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

InfoTypes: 1 of 150 max

Select built-in and custom defined infoTypes to scan for matching data. InfoTypes selected here may be used in hotword and exclusion rules.

BUILT-IN

CUSTOM

Filter

US_SOCIAL_SECURITY_NUMBER

Enter property name or value

X

III

<input checked="" type="checkbox"/>	Name ↑	Description	Availability ?
<input checked="" type="checkbox"/>	US_SOCIAL_SECURITY_NUMBER	A United States Social Security number (SSN) is a 9-digit ...	Any location

DONE

CANCEL

Figure 6 – Leave Defaults before creating.

✓ 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

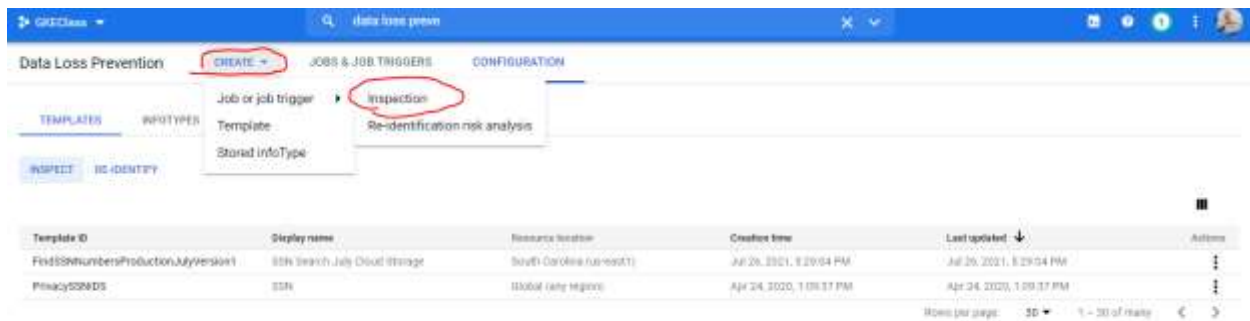
After selecting “Create”

Figure 7 – Inspection Template Details.

← Inspection template details		EDIT	COPY	DELETE
FindSSNNumbersProductionJulyVersion1				
projects/gkeclass1/locations/us-east1/inspectTemplates/FindSSNNumbersProductionJulyVersion1				
Basic info				
Display name	SSN Search July Cloud Storage			
Description	Find SSN Numbers in Cloud Storage			
Built-in infoTypes	US_SOCIAL_SECURITY_NUMBER			
Minimum likelihood	Very likely			
Content types	Unspecified			
Include quote	Off			
Exclude infoTypes	Off			
Create time	Jul 26, 2021, 5:29:04 PM			
Update time	Jul 26, 2021, 5:29:04 PM			

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

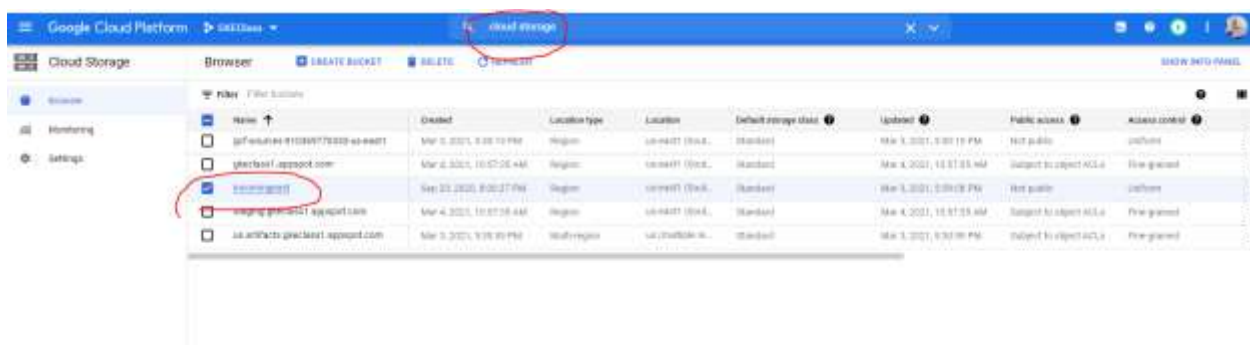


After selecting “Inspection” we know need to ensure we have a Cloud Storage Bucket and Objects to scan.

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.

Bucket details

incomingeast

OBJECTS CONFIGURATION PERMISSIONS RETENTION LIFECYCLE

Buckets > incomingeast

UPLOAD FILES UPLOAD FOLDER CREATE FOLDER MANAGE HOLDS DOWNLOAD DELETE

Filter by name prefix only Filter objects and folders

Name	Size	Type	Created time	Storage class	Last modified	Public access	Encryption
0.jpg	91.2 KB	image/jpeg	Sep 23, 2020, 8:...	Standard	Sep 23, 2020,...	Not public	Google-managed key
1-Certified Secure Software Lifecycle Pn	524.5 KB	image/jpeg	Sep 23, 2020, 8:...	Standard	Sep 23, 2020,...	Not public	Google-managed key
1-Certified Secure Software Lifecycle Pn	524.5 KB	image/jpeg	Sep 23, 2020, 8:...	Standard	Sep 23, 2020,...	Not public	Google-managed key
1-aws (2).jpg	93.6 KB	image/jpeg	Sep 23, 2020, 8:...	Standard	Sep 23, 2020,...	Not public	Google-managed key
2-Blockchain Security Fundamentals.jpg	425.4 KB	image/jpeg	Sep 23, 2020, 8:...	Standard	Sep 23, 2020,...	Not public	Google-managed key
SSNTEST.txt	228 B	text/plain	Jul 26, 2021, 5:4...	Standard	Jul 26, 2021,...	Not public	Google-managed key

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

Select Create

Figure 11 – DLP Configuration

Data Loss Prevention CREATE JOBS & JOB TRIGGERS **CONFIGURATION**

TEMPLATES INFOTYPES

INSPECT DE-IDENTIFY

Template ID	Display name	Resource location
FindSSNNumbersProductionJulyVersion1	SSN Search July Cloud Storage	South Carolina (us-east1)
PrivacySSNIDS	SSN	Global (any region)

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

Figure 12 – Back to DLP Inspection

The screenshot shows the Google Cloud Data Loss Prevention console. At the top, there is a blue header with the 'GKEClass' logo and a search bar labeled 'Search products and resources'. Below the header, the 'Data Loss Prevention' section is active, with a 'CREATE' dropdown menu open. The dropdown menu has three main options: 'Job or job trigger', 'Template', and 'Stored infoType'. The 'Job or job trigger' option is expanded, showing two sub-options: 'Inspection' and 'Re-identification risk analysis'. The 'Inspection' option is selected. Below the dropdown, there are tabs for 'TEMPLATES' and 'INFOTYPES', with 'TEMPLATES' being the active tab. Under 'TEMPLATES', there are buttons for 'INSPECT' and 'DE-IDENTIFY'. Below these buttons is a table with three columns: 'Template ID', 'Display name', and 'Resource location'.

Template ID	Display name	Resource location
FindSSNNumbersProductionJulyVersion1	SSN Search July Cloud Storage	South Carolina (us-east1)
PrivacySSNIDS	SSN	Global (any region)

Enter Select Information as below in Figure 13.

Figure 13- Select Bucket and Location info.

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/dlpsscanssn1

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

Figure 14- Select Template.



Create job or job trigger

to Jobs list



Choose input data



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

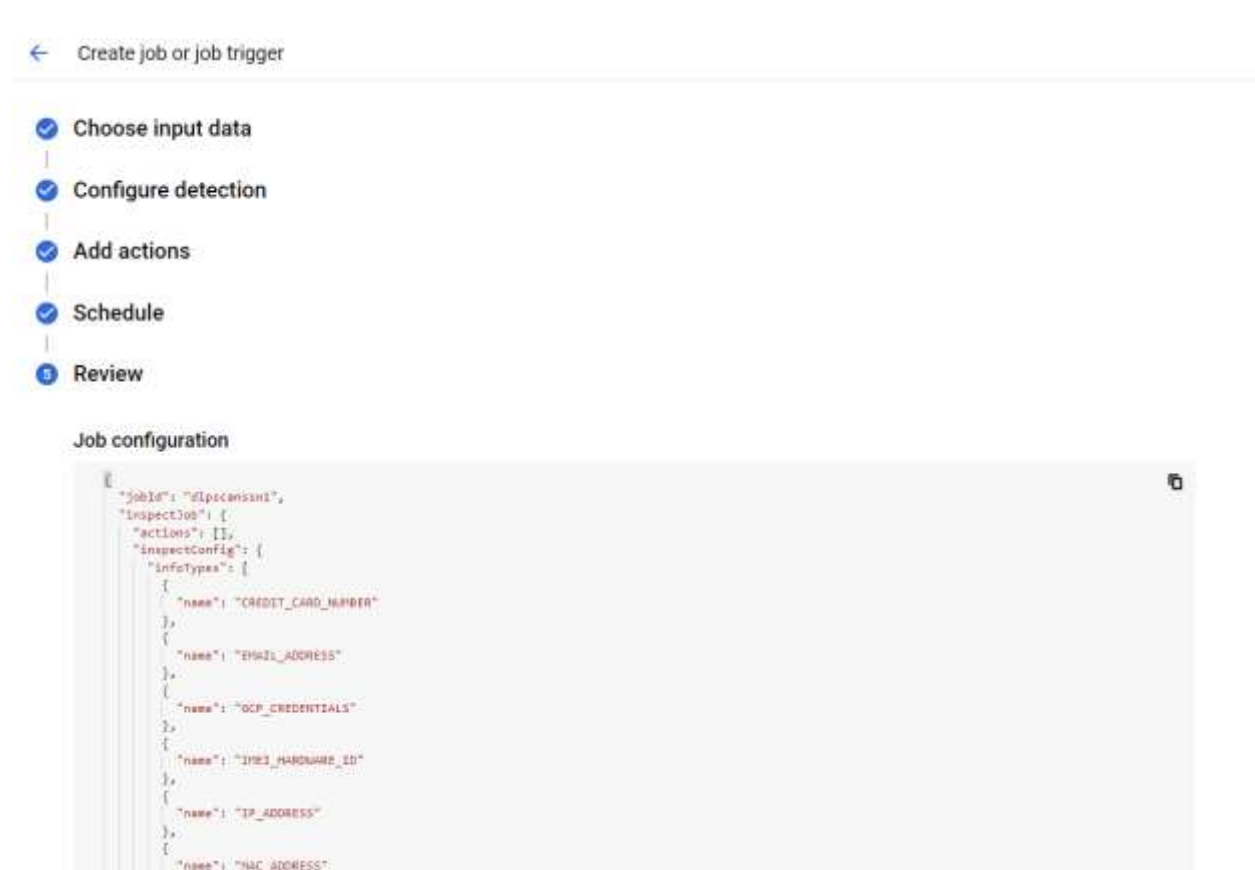
Rows per page: 10 ▼

1 – 10 of 14 < >

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

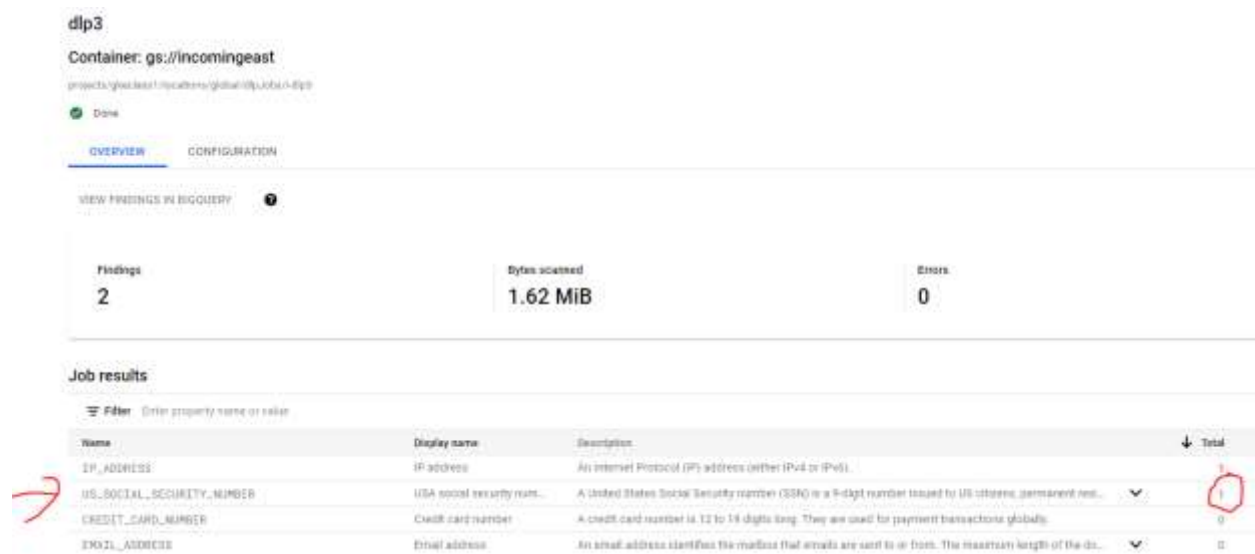
Confirm job or job trigger create

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.