IBM ART Workshop

Applying ART evasion, attacks and defences on image ResNet50 pre-trained DNN (Deep Neural network)

In this notebook we will discover :

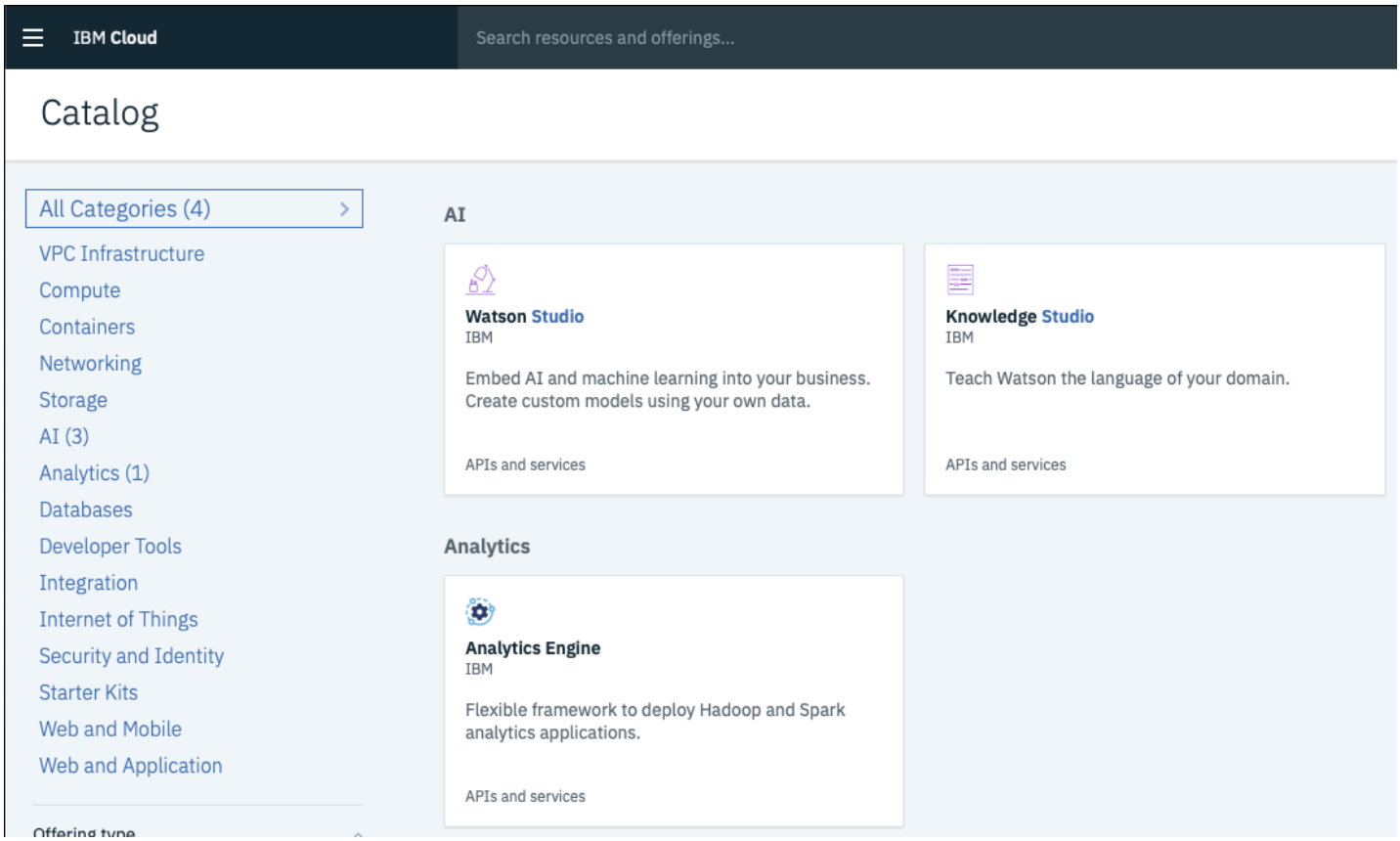
1. How to work with a Keras image classifier in ART
2. How ART actually abstracts from the specific ML/DL backend
3. How to apply a Projected Gradient Descent (PGD) evasion attack against that classifier
4. How to deploy defences against such attacks
5. How to create adversarial samples that can bypass those defences

Chapter 1 : Prerequisites Environment setup

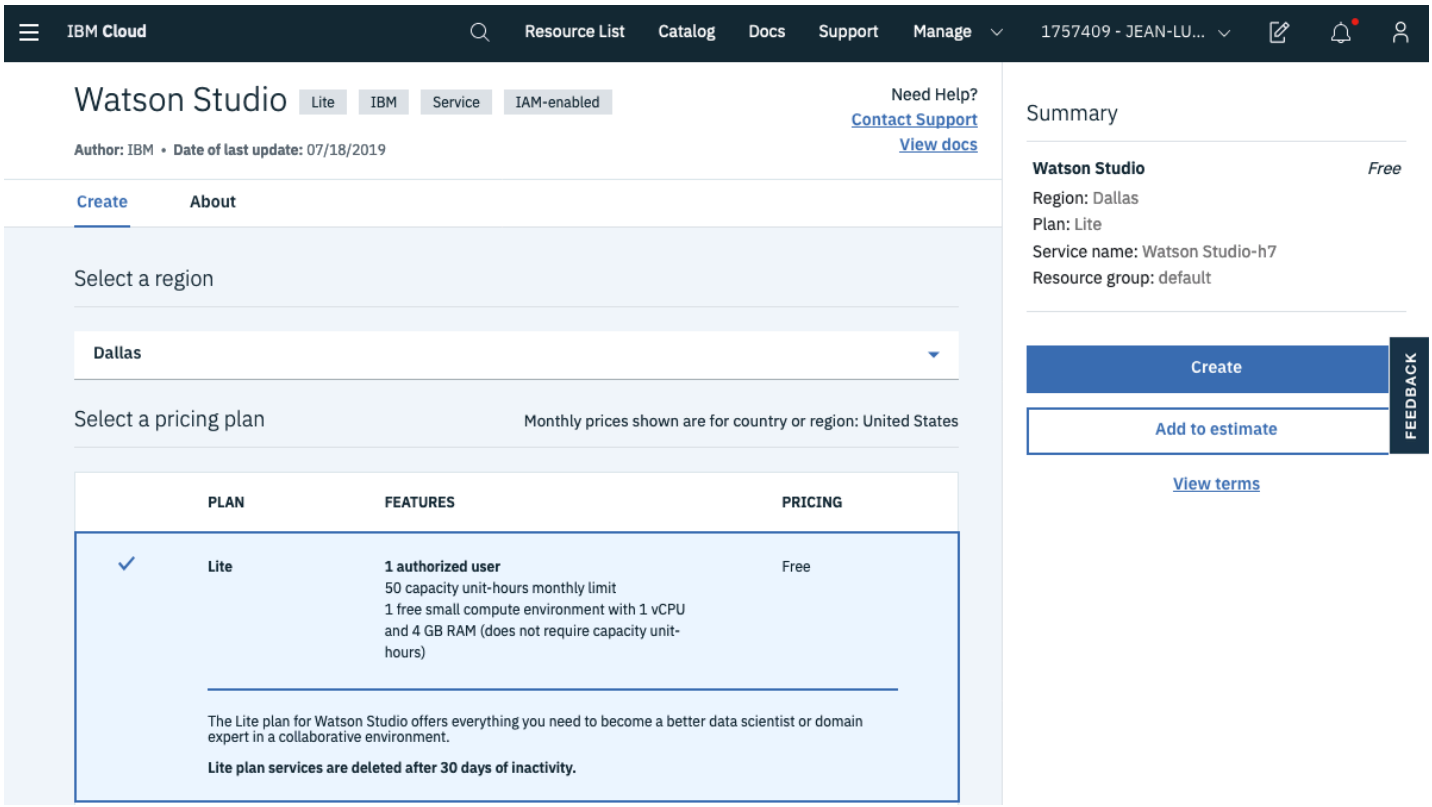
To participate in all components of this lab, you are advised to complete the following prior to attending the hands-on training session.

1. Log in to your IBM Cloud account and provision a Watson OpenScale Lite plan.

To do so please login onto the IBM Cloud website and then search the catalaog for the word **Studio** the follwoing result should appear

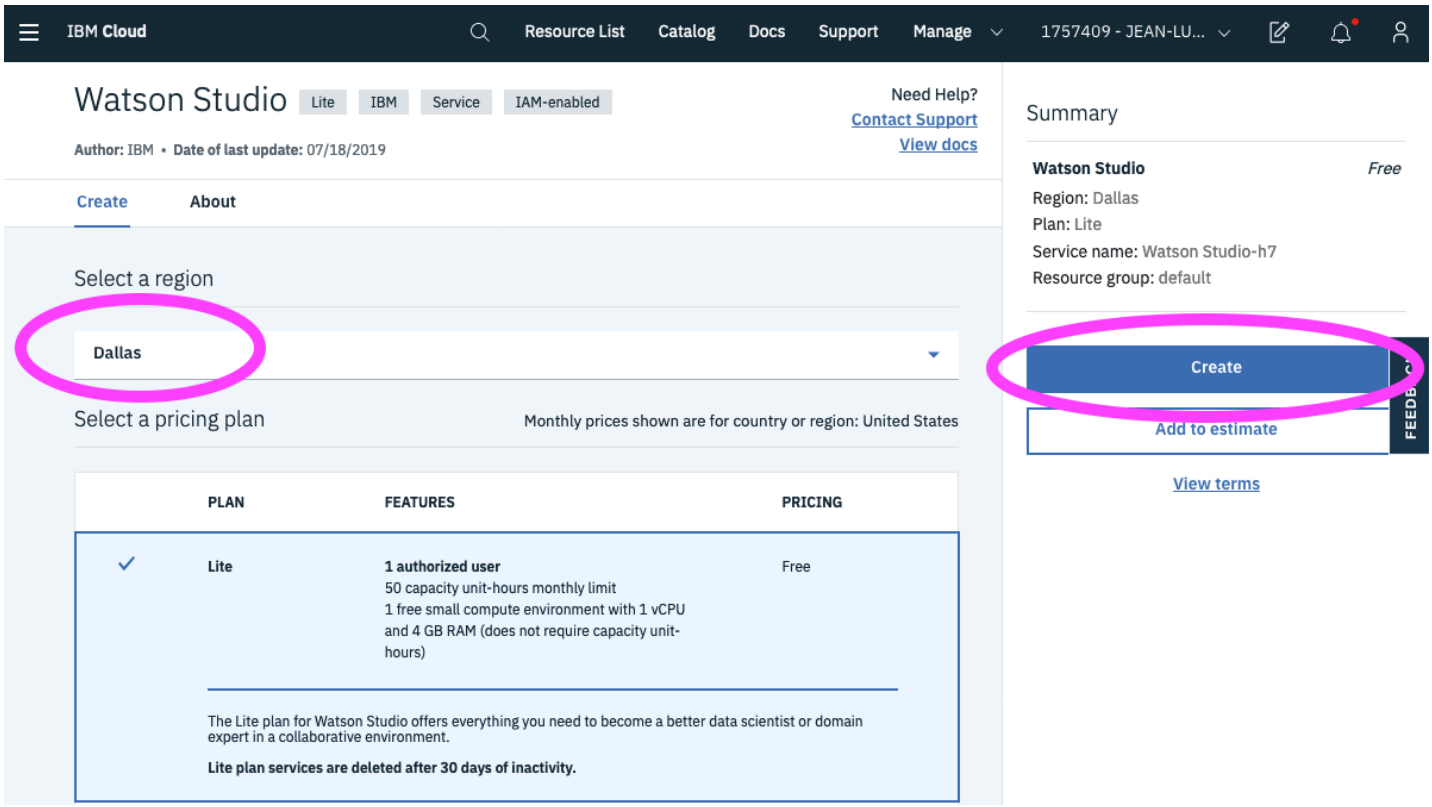


Click on the Watson Studio service

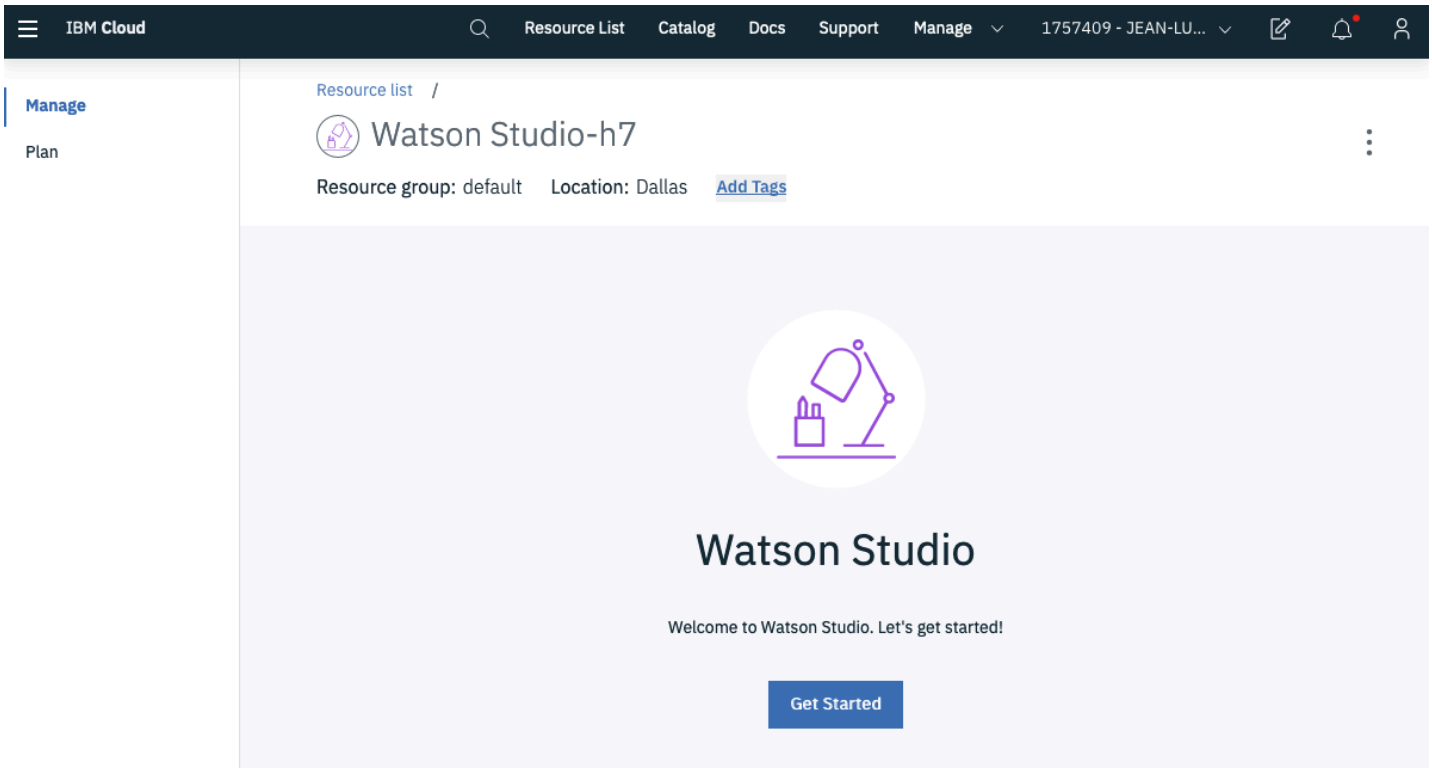


Very important select the Dallas Location to benifit all beta features of the product.

Click the create button.



on the following screen CLick the **Get Started** button to launch Watson Studio app.

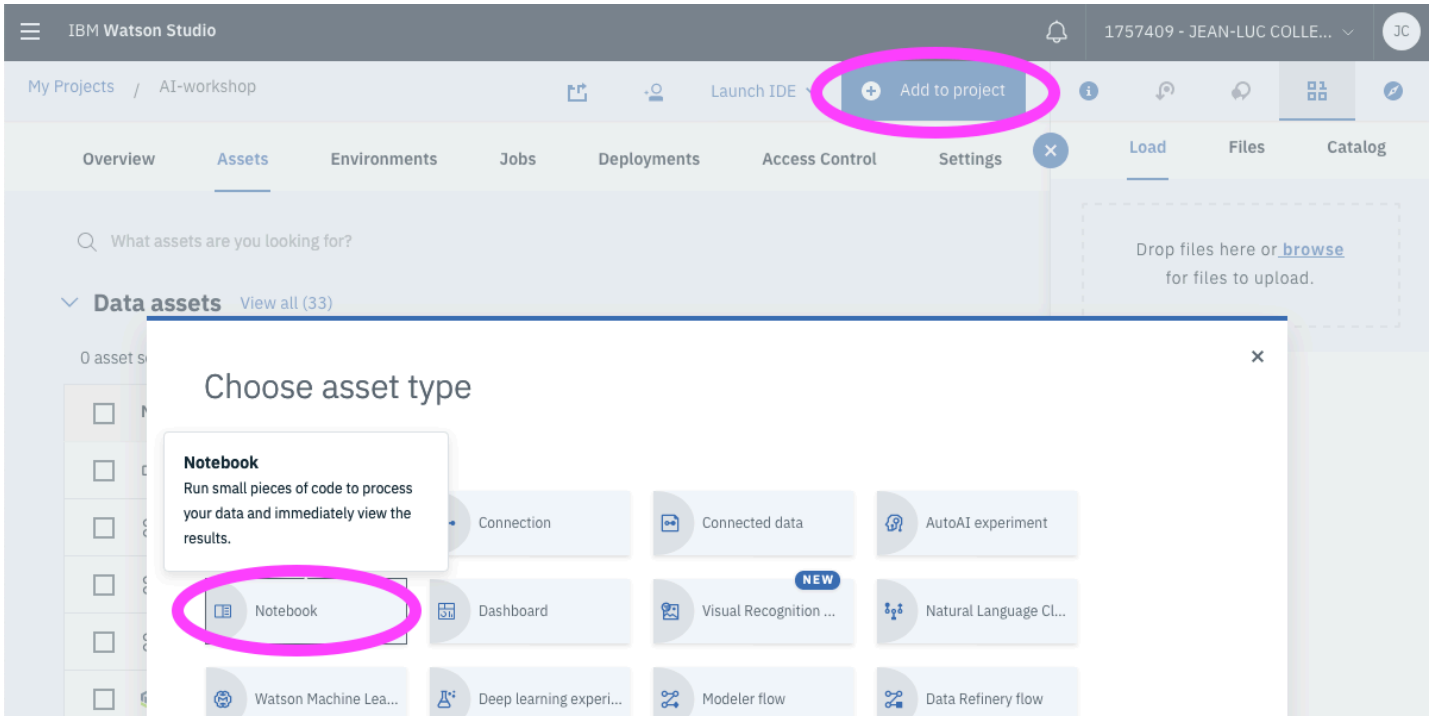


At the application startup create a new project or re-use an existing one.

Download on your local system the file called **'ART Attack-Defense.ipynb'** from the box Lab folder

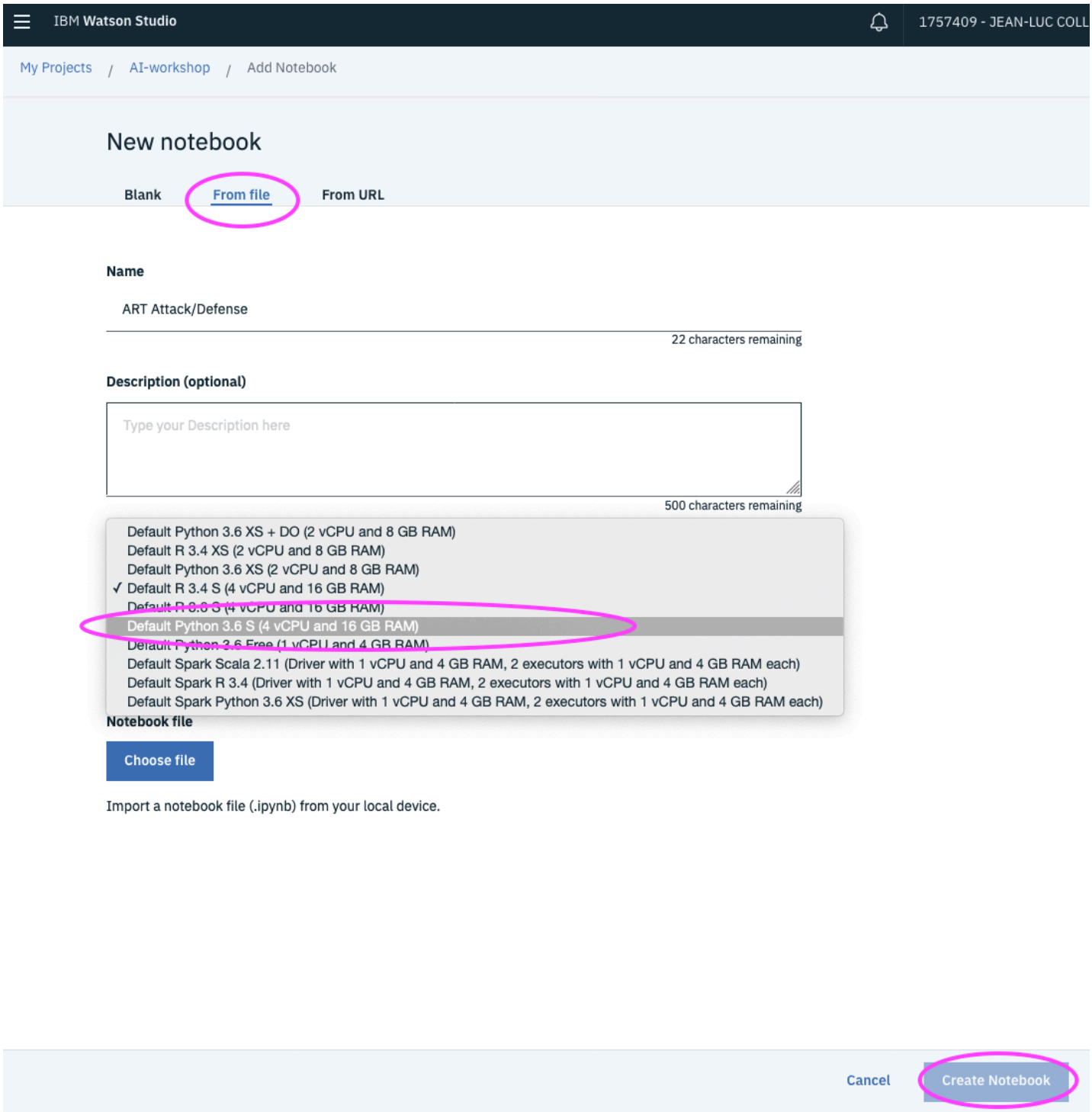
Then from your project environment click on the "Add to Project Button" and select Notebook to create a

new Jupiter notebook environment as shown below



From the creation form of the new notebook Give a name to your project here I choosed **ART-Attack-Defense** then Click the **From File** Tab and for better performance select the **Python S** preset env (not mandatory but recommended !).

click **Choose File** button and select the **ART Attack-Defense.ipynb** notebook file you downloaded earlier from the box folder.



When satisfied, click Create Notebook to generate the environment.

Run the notebook cell by cell and see what's happening or from the menu select **Cell>>Run All** and follow the notebook commnents & outputs.

Hope you njoy the lab !!!

Jean-Luc Collet

http://fr.linkedin.com/pub/jean-luc-collet

Thanks !

Nov 1th, 2019