

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 catalog for the word **Studio** the following result should appear

Search resources and offerings...

Catalog

All Categories (4) >

VPC Infrastructure
Compute
Containers
Networking
Storage
AI (3)
Analytics (1)
Databases
Developer Tools
Integration
Internet of Things
Security and Identity
Starter Kits
Web and Mobile
Web and Application

AI

Watson Studio
IBM

Embed AI and machine learning into your business.
Create custom models using your own data.

APIs and services

Knowledge Studio
IBM

Teach Watson the language of your domain.

APIs and services

Analytics

Analytics Engine
IBM

Flexible framework to deploy Hadoop and Spark analytics applications.

APIs and services

Click on the Watson Studio service

Resource List
Catalog
Docs
Support
Manage
1757409 - JEAN-LU...

Watson Studio
Lite
IBM
Service
IAM-enabled

Need Help?
[Contact Support](#)
[View docs](#)

Author: IBM • Date of last update: 07/18/2019

Create About

Select a region

Dallas

Select a pricing plan
Monthly prices shown are for country or region: United States

PLAN	FEATURES	PRICING
✓ Lite	1 authorized user 50 capacity unit-hours monthly limit 1 free small compute environment with 1 vCPU and 4 GB RAM (does not require capacity unit-hours)	Free

The Lite plan for Watson Studio offers everything you need to become a better data scientist or domain expert in a collaborative environment.
Lite plan services are deleted after 30 days of inactivity.

Summary

Watson Studio *Free*
Region: Dallas
Plan: Lite
Service name: Watson Studio-h7
Resource group: default

Create

Add to estimate

[View terms](#)

FEEDBACK

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

Click the create button.

IBM Cloud

Resource List Catalog Docs Support Manage 1757409 - JEAN-LU...

Watson Studio

Lite IBM Service IAM-enabled

Author: IBM • Date of last update: 07/18/2019

Need Help? [Contact Support](#) [View docs](#)

Create About

Select a region

Dallas

Select a pricing plan Monthly prices shown are for country or region: United States

PLAN	FEATURES	PRICING
✓ Lite	1 authorized user 50 capacity unit-hours monthly limit 1 free small compute environment with 1 vCPU and 4 GB RAM (does not require capacity unit-hours)	Free

The Lite plan for Watson Studio offers everything you need to become a better data scientist or domain expert in a collaborative environment.

Lite plan services are deleted after 30 days of inactivity.

Summary

Watson Studio Free

Region: Dallas
 Plan: Lite
 Service name: Watson Studio-h7
 Resource group: default

Create

Add to estimate

[View terms](#)

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

IBM Cloud

Resource List Catalog Docs Support Manage 1757409 - JEAN-LU...


Manage

Plan

Resource list /

Watson Studio-h7

Resource group: default Location: Dallas [Add Tags](#)



Watson Studio

Welcome to Watson Studio. Let's get started!

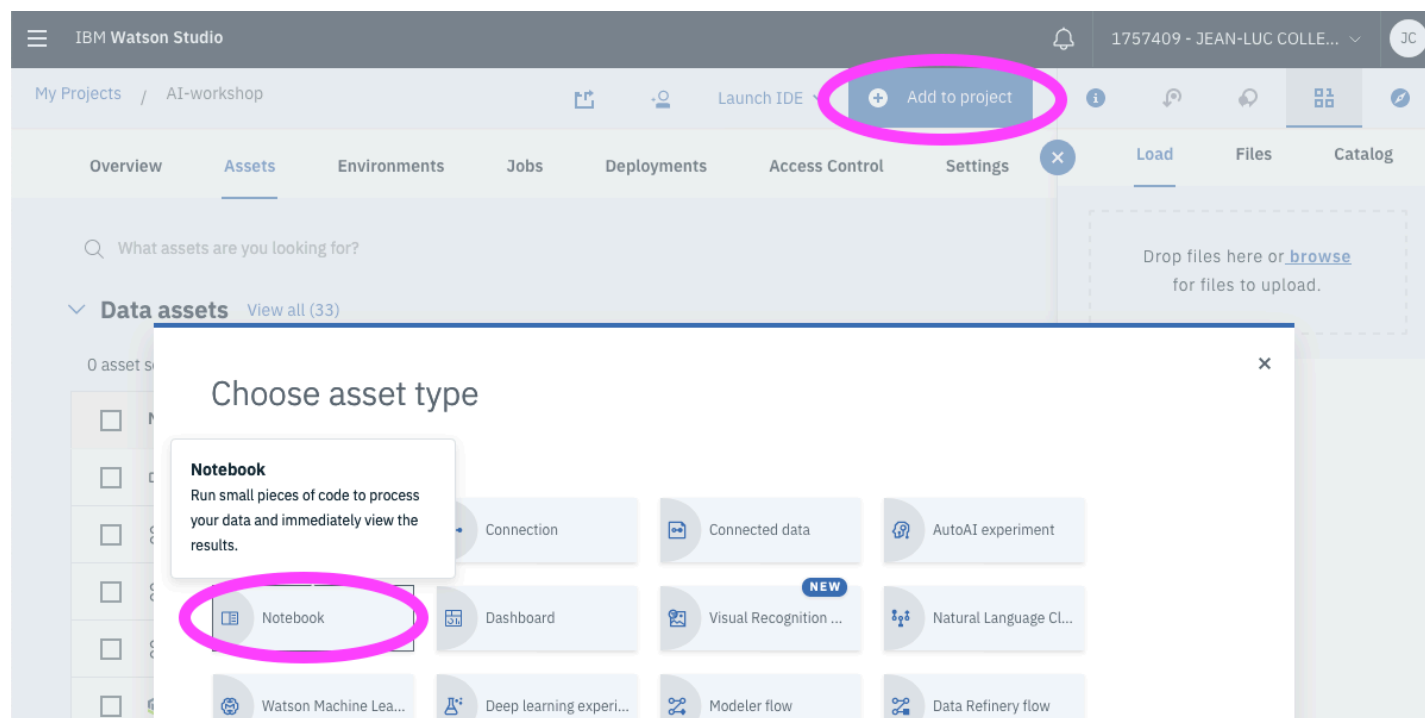
Get Started

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.

IBM Watson Studio

1757409 - JEAN-LUC COLL

My Projects / AI-workshop / Add Notebook

New notebook

Blank From file From URL

Name
ART Attack/Defense
22 characters remaining

Description (optional)

Type your Description here

500 characters remaining

Default Python 3.6 XS + DO (2 vCPU and 8 GB RAM)

Default R 3.4 XS (2 vCPU and 8 GB RAM)

Default Python 3.6 XS (2 vCPU and 8 GB RAM)

✓ Default R 3.4 S (4 vCPU and 16 GB RAM)

Default R 3.6 S (4 vCPU and 16 GB RAM)

Default Python 3.6 S (4 vCPU and 16 GB RAM)

Default Python 3.6 Free (1 vCPU and 4 GB RAM)

Default Spark Scala 2.11 (Driver with 1 vCPU and 4 GB RAM, 2 executors with 1 vCPU and 4 GB RAM each)

Default Spark R 3.4 (Driver with 1 vCPU and 4 GB RAM, 2 executors with 1 vCPU and 4 GB RAM each)

Default Spark Python 3.6 XS (Driver with 1 vCPU and 4 GB RAM, 2 executors with 1 vCPU and 4 GB RAM each)

Notebook file

Choose file

Import a notebook file (.ipynb) from your local device.

Cancel

Create Notebook

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 comments & outputs.

Hope you enjoy the lab !!!



[Jean-Luc Collet](#)

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

Thanks !

Nov 1th, 2019