EVIDEN

07 Wrap up and openings

Data security

Identities management in code

Lab

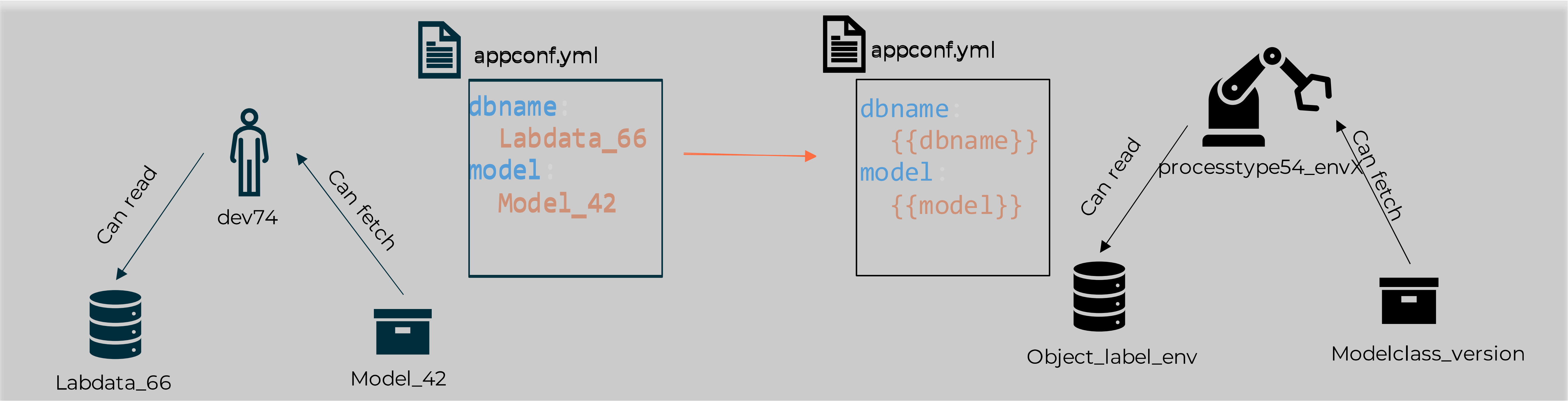
Applications / pipelines run on your name, or on project name

Externalize

- DB connections credentials
- Storage credentials
- Registries (artifact, containers, models)
- Other specific credentials (shell, processing tools accounts)

Production

Code run on service accounts

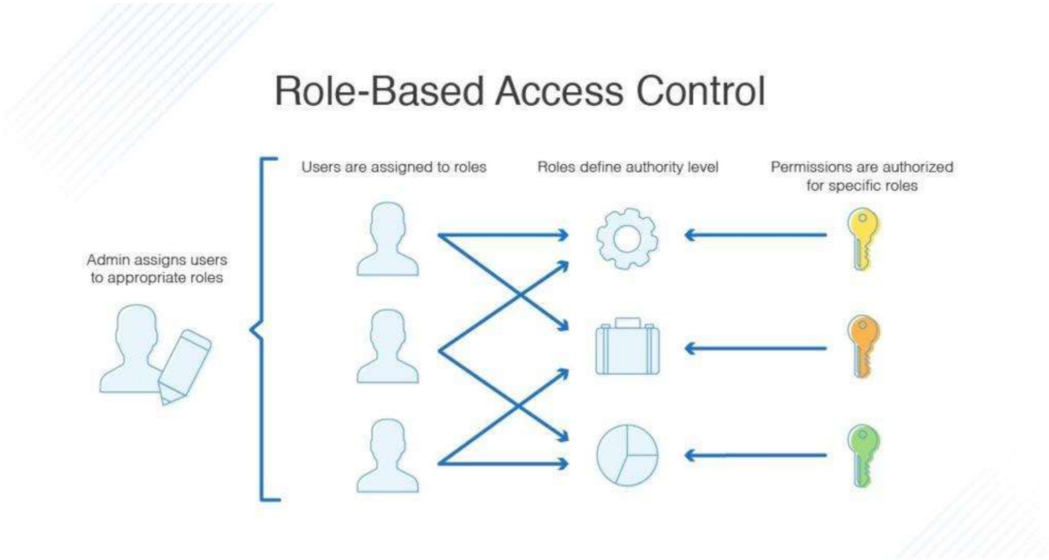


```
dbname:
  Labdata_66
model:
  Model_42
```

```
dbname:
  {{dbname}}
model:
  {{model}}
```

Data security

Authorization policies : RBAC vs ABAC

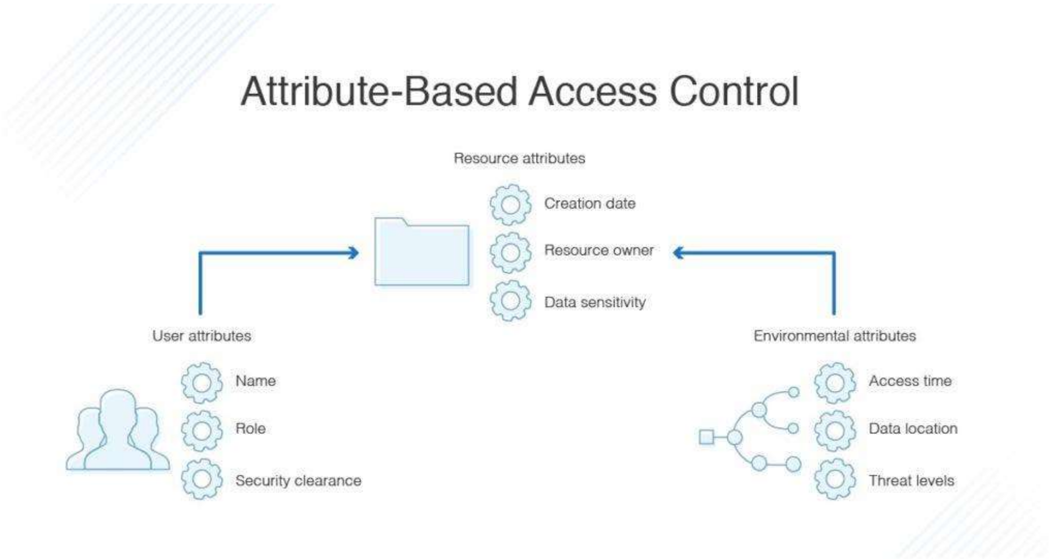


Role-Based Access Control
Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

Administrator define roles : (dwh viewer, report viewer, pipeline maintainer)

A **user** is assigned to a set of roles through groups

Roles define a set access (r/w) on some objects (files/ db)



User, Resources and Environment got **attributes.**

Rules define which attribute combinations are authorized in order for the user to successfully perform an action with the object.

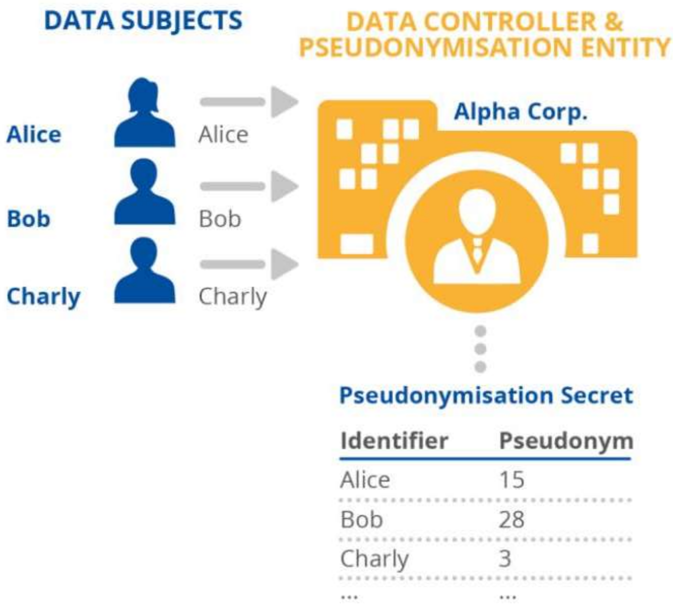
Mix Authorization policy with :

Broad access enforcer by RBAC
Complex access by ABAC

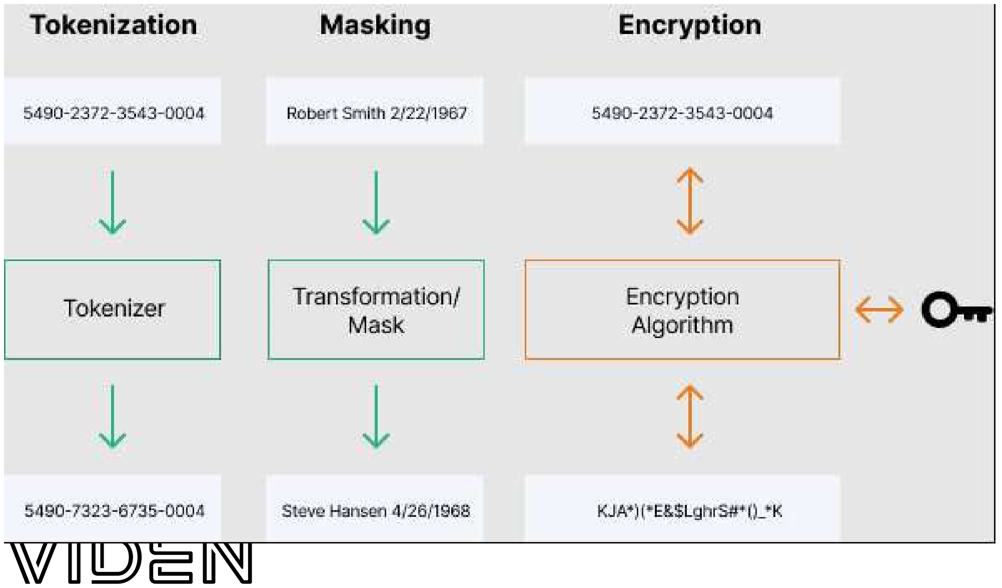
Data security

Data protection

Transform data to preserve sensitive informations



Identifier	Pseudonym
Alice	15
Bob	28
Charly	3
...	...



Pseudonymisation :

techniques that replace, remove or transform information that identifies individuals, and keep that information separate

Obfuscation :

techniques for transforming data into a different form to protect it

ML applications do not need whole or row data to be efficient, apply ML on pseudonymised / obfuscated data to preserve security

API Management

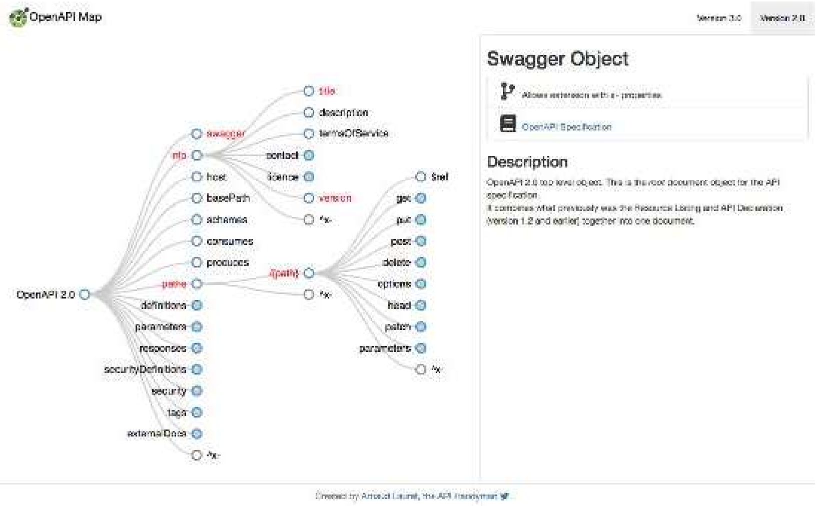
Introduction

API : stricto sensu it's only the interface, but usually it defines all the layers behind (Interface, business logic, data)

API Management : it's a set of processus and tools that manage and secure APIs and services. It enables developers to work with APIs more effectively by providing features such as authentication, access control, analytics and monitoring

Application Programming Interface

Spec



Swagger Object

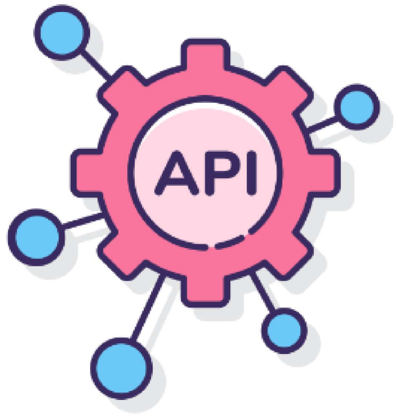
Allows extension with x- properties.

OpenAPI Specification

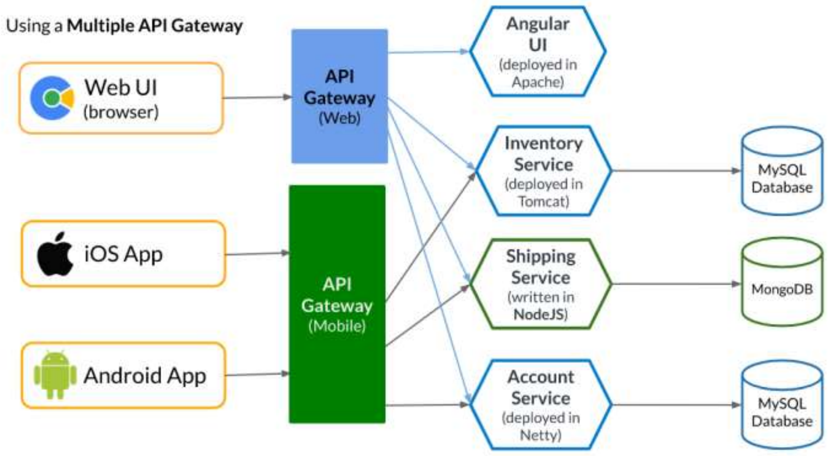
Description

OpenAPI 2.0 top level object. This is the root document object for the API specification.
It combines what previously was the Resource Listing and API Declaration (version 1.2 and earlier) together into one document.

Created by Arnaud Lauret, the API Handyman



Manager

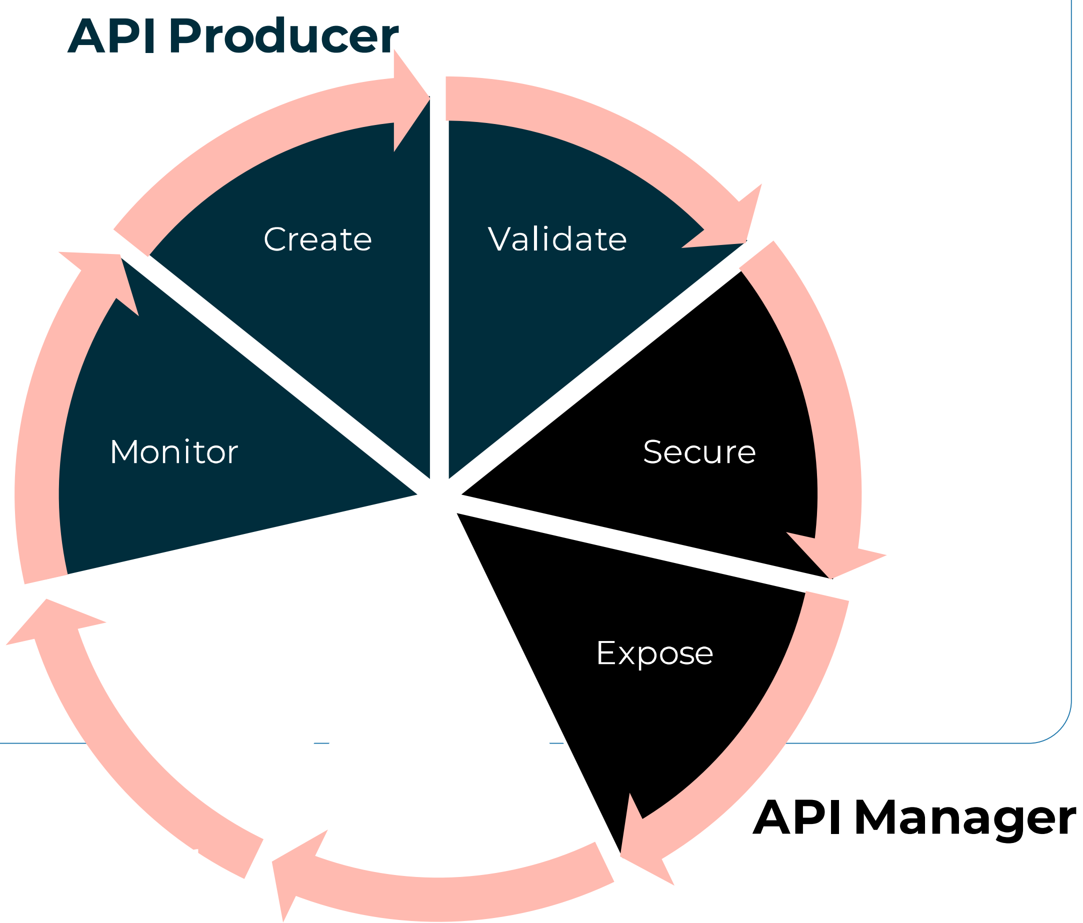


API Management

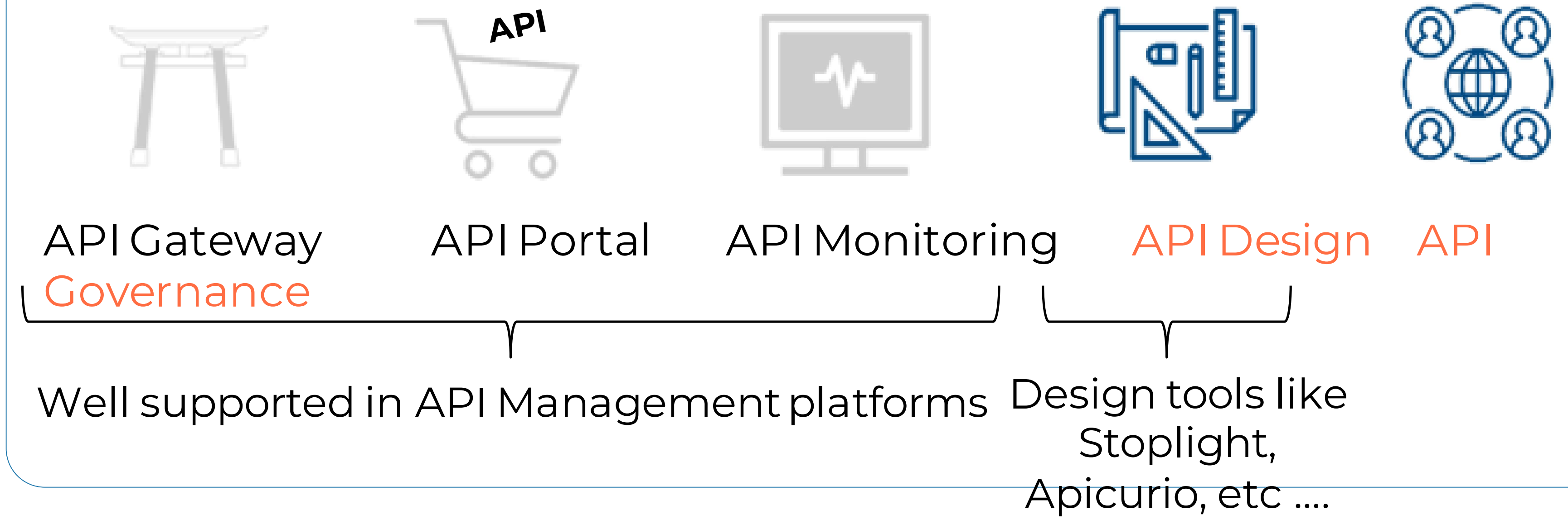
Roles and Pillars

Full API Lifecycle management is a **key challenge** for digital business enablement

3 **roles** in the API lifecycle



5 **pillars** for handling the API lifecycle



API Management

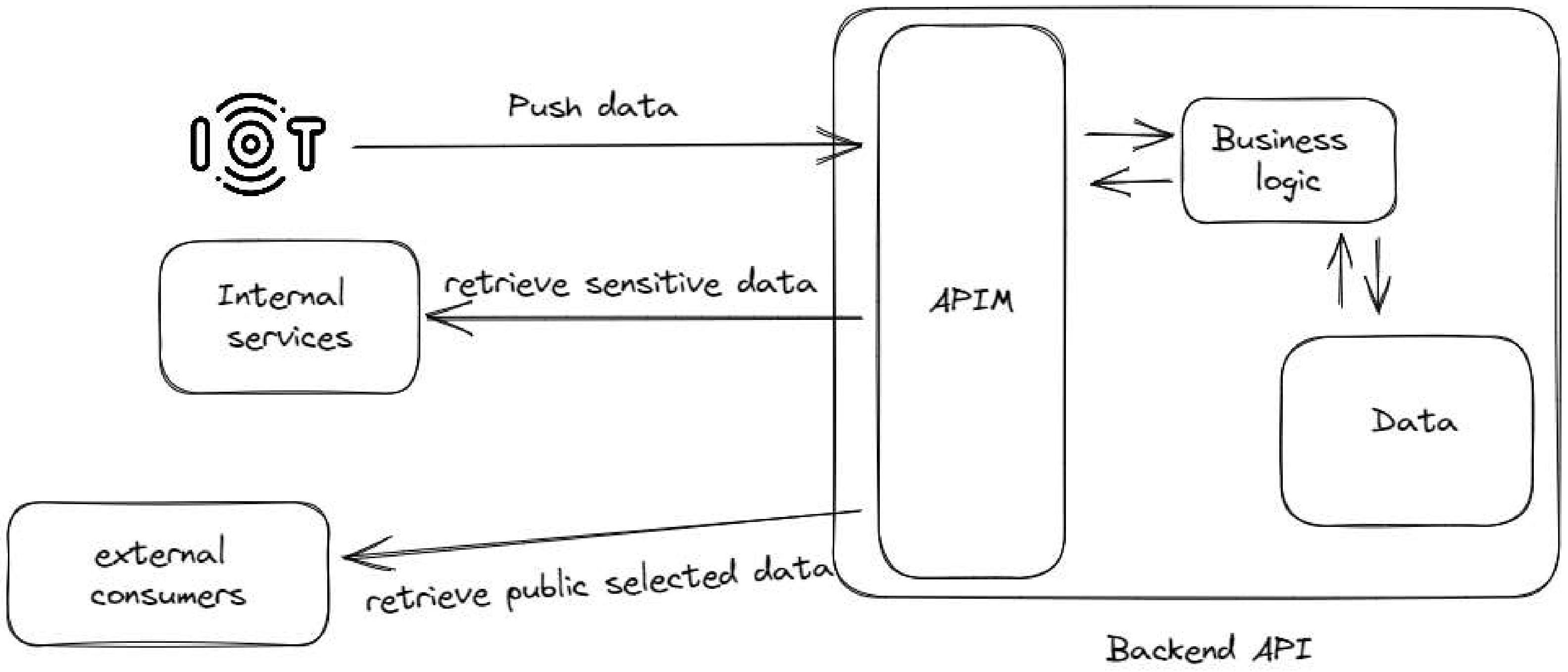
Focus Data

- How to expose securely and monitor my data both internally and publicly ?
  → API Management is a strong tool to expose your data

- Control the access to your data depending on your consumer.

- Choose the resources to expose internally and externally and how to access it (read, write, update etc …)

- Monitor your APIs consumption and prevent attacks on your backends



Financial market data for trading

Pushing and retrieving data from sensors

Enabling third-party developers to build new applications

EVIDEN

API Management

Focus AI/ML

- AI/ML Apis are often slow APIs that consume a lot of the backend resources.

  → API Management can secure these backends by applying some traffic rules

- Traffic Management allows to define quotas and spike arrest

- Monitoring and Analytics: API management tools can provide monitoring and analytics capabilities to track usage patterns, identify performance bottlenecks, and monitor the quality of AI/ML predictions.

Example of AI APIs behind Api Gateway

LLM models for chat / QA / retrieval

Image recognition APIs for CCTV cameras

Image to text APIs

Open Data

Opportunities from transparency

- From USA government original initiative
  - Make institution feel more trustable
  - Allow external services to use this data to create value

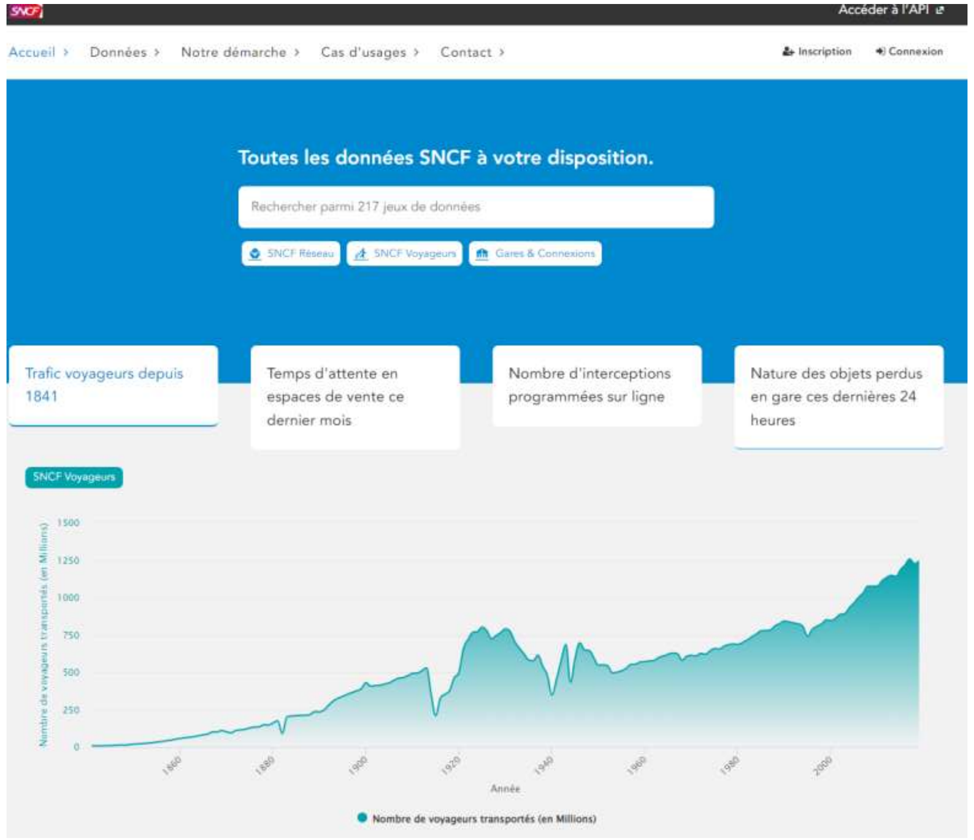
- All European institution have to “liberate” some data

Now transposed to companies as

“open innovation”

“data marketplace”

Based on data catalog – api managers



Toutes les données SNCF à votre disposition.

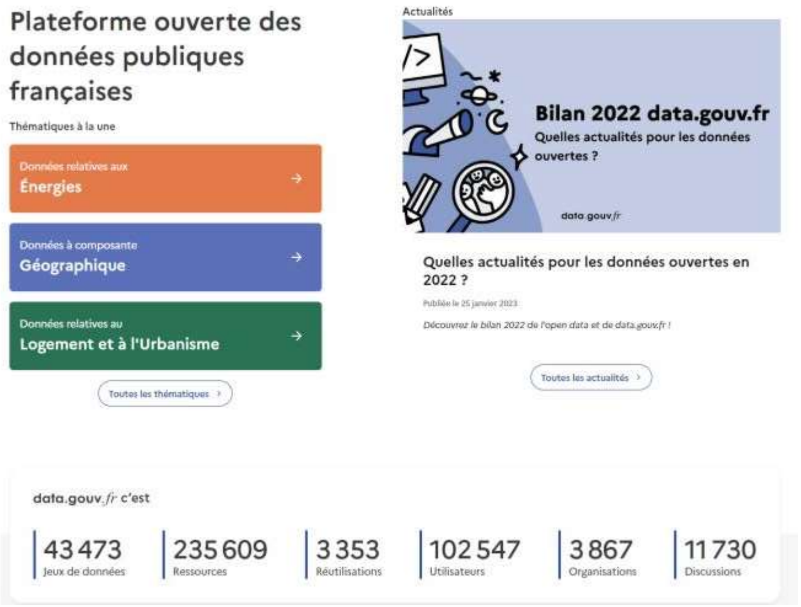
Trafic voyageurs depuis 1841

Temps d'attente en espaces de vente ce dernier mois

Nombre d'interceptions programmées sur ligne

Nature des objets perdus en gare ces dernières 24 heures

SNCF Voyageurs
Nombre de voyageurs transportés (en Millions)
1500
1250
1000
750
500
250
0
1860
1880
1900
1920
1940
1960
1980
2000
Année
Nombre de voyageurs transportés (en Millions)



Plateforme ouverte des données publiques françaises

Thématiques à la une

Quelles actualités pour les données ouvertes en 2022 ?

Publiée le 25 janvier 2023

Découvrez le bilan 2022 de l'open data et de data.gouv.fr !

data.gouv.fr c'est

43 473	235 609	3 353	102 547	3 867	11 730
Jeux de données	Ressources	Réutilisations	Utilisateurs	Organisations	Discussions

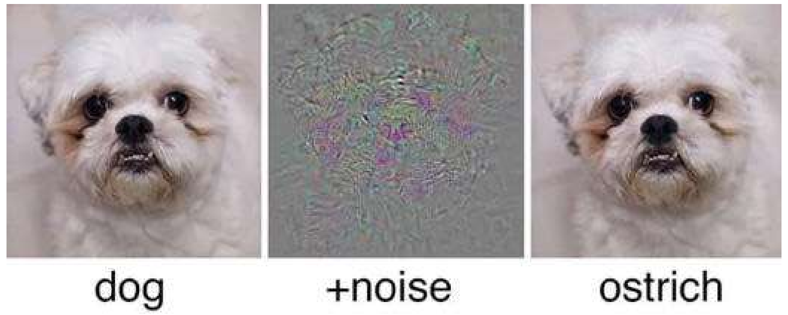
Explainability

Why do we need it and what we want

Biases

- COMPAS algorithm in the US for predicting criminal reoffending was biased toward black people
- 2018, 3 of the latest gender-recognition were essentially working for white people. Risk of false identification for women and minorities
- 2015 study showing the Google search for CEO and advertisement for high-income jobs were biased towards men
- October 2017, Palestinian worker arrested because he had allegedly posted « attack them » on Facebook while he had written « good morning ». Facebook algorithm translated it badly
- PredPol is an algorithm predicting when and where crimes take place. The algorithm unfairly targeted certain neighborhoods

Adversarial example



Every algorithm could fail, to be able to trust them we need proofs, éléments that helps us understand the model output

Trust

Confidence of well performance, understanding of the model (white-box), for which example it is right => avoid that mistakes are being made in some regions (black people for instance)

Causality

Though ML is based on associations, one might hope to infer causal relationships

Robustness

We want to ensure that ML models generalize well
Eg: Adversarial example

Informativness

What we want here is to explore data more precisely

Ethics & law

One wants to be one step ahead of regulation and try to develop a way to challenge algorithmic decision

Explainability

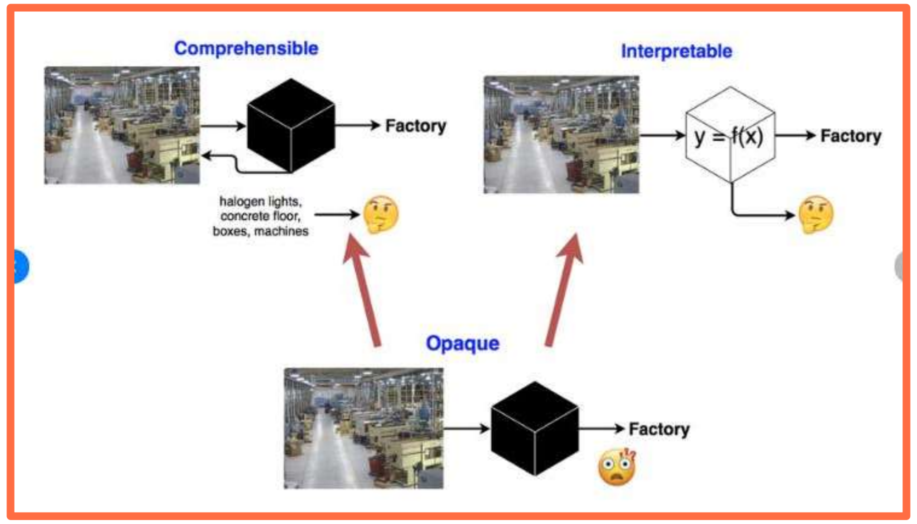
Definition

Synonymes

- Some use interchangeably the terms **explainable AI** and **interpretable AI**
- Others differentiate between **comprehensible** and **interpretable AI**

Explainability provides a line of reasoning, answering the why of the decision-making process in human-understandable terms.

Comprehensibility
(post-hoc interpetation)



Interpretability
(algorithm transparency)

Emit symbols (words, visualizations) for the user of the ML system to relate properties of the inputs to their output

Eg: t-SNE is comprehensible since it allows to relate properties of the input to the output but not interpretable since the user does not understand clearly the relationship between input and output

When the user can understand how inputs are mapped to outputs, the system is said to be interpretable

Eg : a linear regression is interpretable because the user can compare the covariates' weights to see their relative importance in the prediction

Understandabilit y

Low interpretability

Error function is nonlinear and nonmonotonic
Eg: neural networks

Medium interpretability

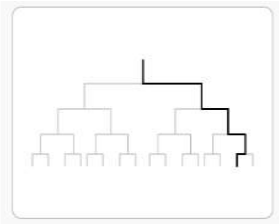
Error function is nonlinear and monotonic
Eg: logistic regression

High interpretability

Error function is linear and monotonic
Eg: least square regression

Explainability

Global, local, model agnostic, specific XAI



Local interpretability

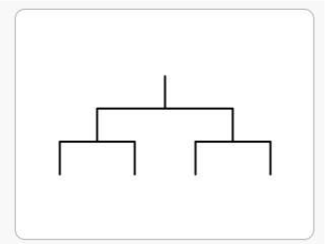
A model is said to be locally interpretable if it is interpretable for a group of similar instances.

Eg: LIME (Local Interpretable Model-agnostic Explanations)

Model agnostic

A model agnostic technique can be applied to different algorithms
Eg: LIME (Local Interpretable Model-agnostic Explanations)

Model agnosticism is convenient but often relies on surrogate models or other approximations that can degrade the accuracy of the explanations provided.



Global interpretability

A model is said to be globally interpretable if one can understand the algorithm itself, the results or the machine learned relationship between the prediction target and the input variables

Eg : decision trees, SLIM (Supersparse Linear Integer Models), global variable importance

Model specific

A model specific technique is applicable to only one algorithm
Eg: treeinterpreter for decision tree, linear regression is a white bow model; meaning that it is readily interpretable

Uses the model to be interpreted directly and thus make potentially more accurate explanations.

Explainability

Lots of technics

https://christophm.github.io/interpretable-ml-book

Model agnostic

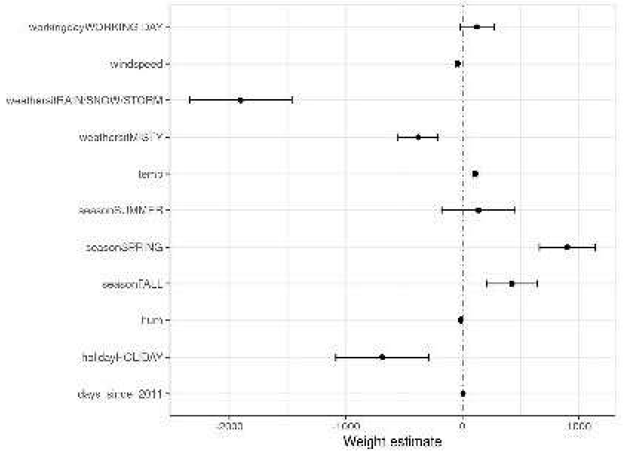
<u>Global Model-agnostic methods</u>
Partial Depence Plot (PDP)
Accumulated Local Effects (ALE)
Feature interaction
Functional Decomposition
Permutation feature importance
Global surrogate

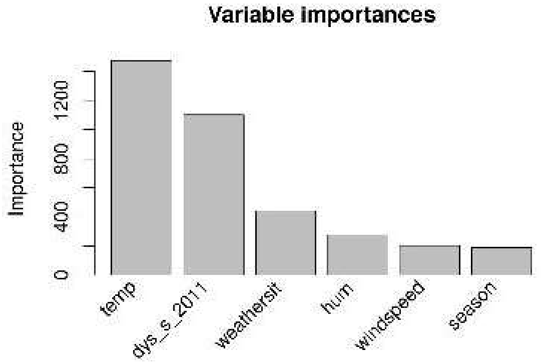
<u>Local Model-agnostic methods</u>
Individual Conditional Expectation (ICE)
Local Surrogate (LIME)
Counterfactual Explanations
Scoped Rules (Anchors)
Shapley Values
Shapley Additive explanation (SHAP)

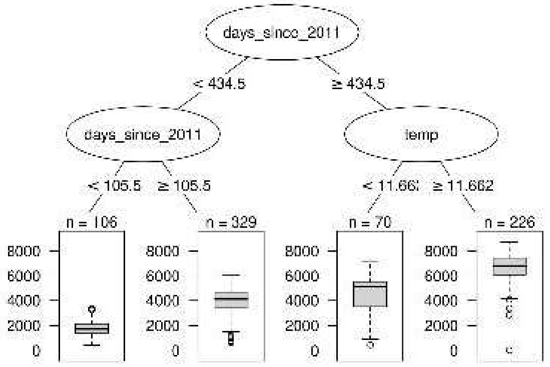
<u>Neural Net methods</u>
Learned features
Pixel Attribution (Saliency Map)
Detecting Concepts
Adversarial Examples

Model specific

<u>Models => explainer</u>
Linear regression => weight plot
Logistic regression
GLM, GAM
Decision Tree => boxplot
Decision Rules
RuleFit => variable importance


workingdayWORKING DAY
windspeed
weathersitRAIN/SNOW/STORM
weathersitMISTY
temp
seasonSUMMER
seasonSPRING
seasonFALL
hum
holidayHOLIDAY
days_since_2011
Weight estimate


Variable importances
Importance
temp
days_since_2011
weathersit
hum
windspeed
season


days_since_2011
< 434.5
≥ 434.5
days_since_2011
temp
< 105.5
≥ 105.5
< 11.662
≥ 11.662
n = 106
n = 329
n = 70
n = 226