La lutte contre la fraude

Evolutions

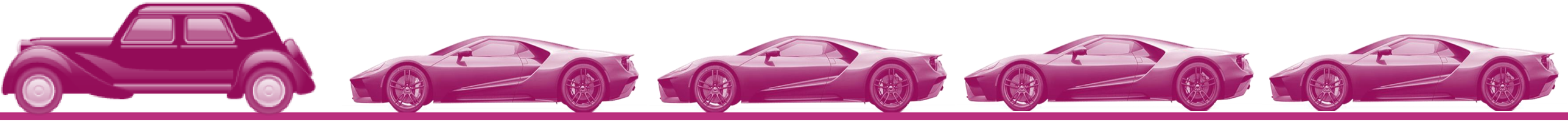
Défis

Solutions

EIFR - 26 février 2020

Avant de commencer…deux truismes…

La solidité d’une chaîne est égale à celle de son maillon le plus faible



La rapidité d’un convoi est égale à celle de son élément le plus lent

La fraude en quelques chiffres

Proportion d’entreprises qui déclarent avoir été victimes de fraude*

2009

30%

2018

49%

* PWC Global Economic Crime and Fraud Survey 2018

La fraude en quelques chiffres

Pression sur les données

Depuis 2005 (et jusqu'au 14 novembre 2019)

9 361 vols massifs de données

11 613 milliards d'enregistrements*

291 enregistrements/sec **

…en comptant seulement les vols massifs…

…donc en ne comptant pas les cas individuels de phishing…

* source: www.privacyrights.org
** source: Malwarebytes

La fraude en quelques chiffres

L’impact du Phishing

32% des **fuites de données** sont liées à du phishing*

* Verizon - Data Breach Investigation Report - 2019

3,4 milliards d’emails de phishing envoyés **chaque année***

* Valimail – Email Fraud Landscape – Spring 2019

1,5 millions de sites de phishing créés **chaque jour***

* Dashlane - Blog

30% des emails de phishing sont **ouverts***

70% en cas de spear phishing

- Verizon - Data Breach Investigation Report – 2016

Problématique fraude pour les établissements bancaires et financiers

Usurpation d’identité

Utilisation d’identifiants volés (login + pwd)

Utilisation d’identités synthétiques

Fourniture d’informations fausses

Accès frauduleux

Ouverture de comptes frauduleux

Accès frauduleux à des comptes légitimes

Objectifs et défis

→ **Réduction de l’impact des fraudes sur les résultats**

→ **Couverture complète, process et canaux (web et app)**

→ **Amélioration du cadre opérationnel de la LCLF**

→ **Préservation et optimisation de l’expérience client**

Caractéristiques d’une approche efficace de la LCLF

Approche technique

Mode **Saas**

Accès via **API unique** flexible

Disponible sur tous les **canaux**

Traitement en **temps réel**

Interface de gestion et investigation

Approche fonctionnelle

Analyse du **device**

Vérification **documentaire** (+KYC)

Analyse de **comportement digital**

Evaluation d’**email**

Jeux de **règles** et **modèles** spécifiques

Concepts de règles **variés**

- Vélocité
- Incohérence
- Listes négatives

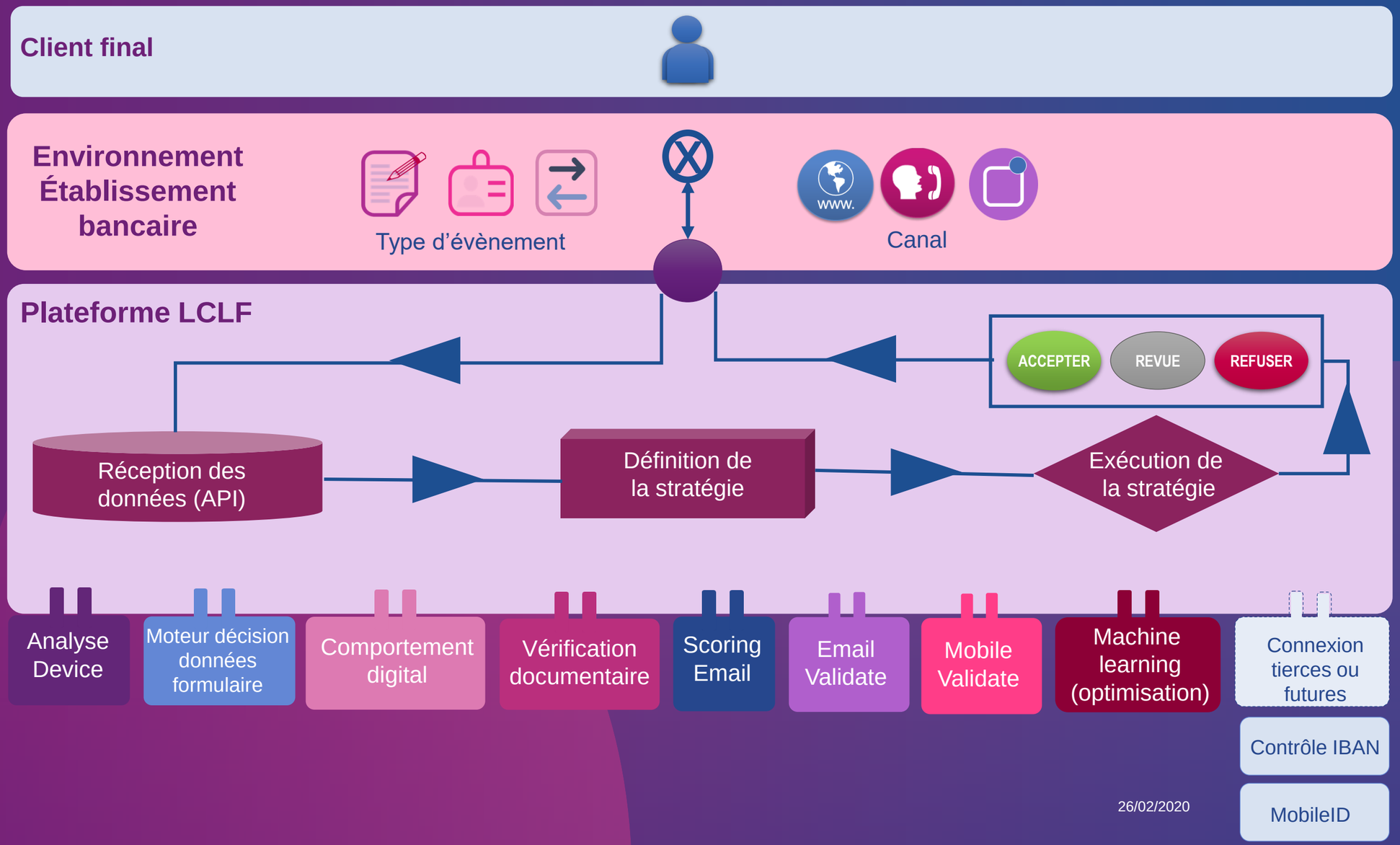
Analyse de **liens**

Modèles optimisés par **Machine Learning**

Un écosystème et une plateforme LCLF

“Se doter des moyens d’analyser tous les points de données clients”

Le concept de plateforme ouverte



FOCUS TECHNO
“Device intelligence”

Qu’est-ce que le device intelligence?

1. Collecte de données fournies passivement par un appareil connecté pendant une session web

2. Traitement de ces données pour créer une identité unique de l’appareil connecté

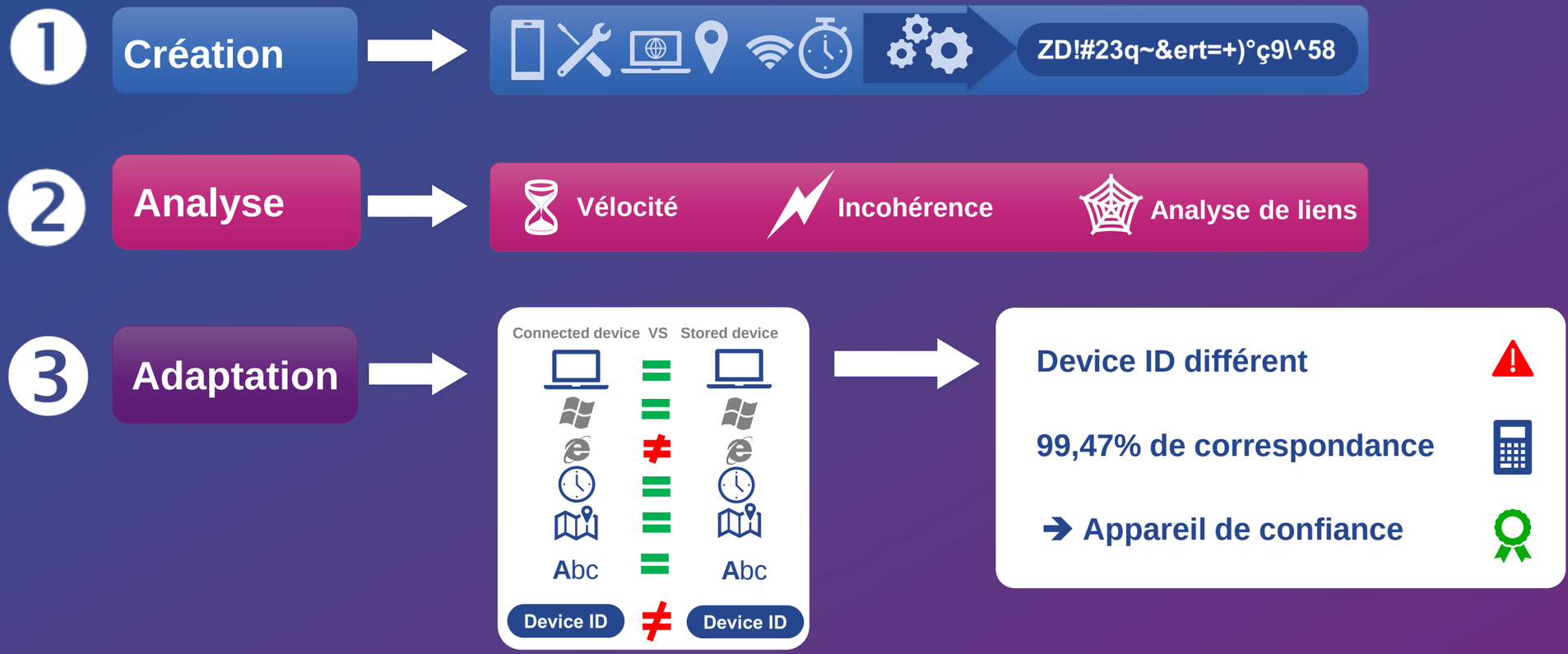
3. Analyse, et exploitation de cette identité via un ensemble de règles, dans un processus donné

Quelles données sont collectées?

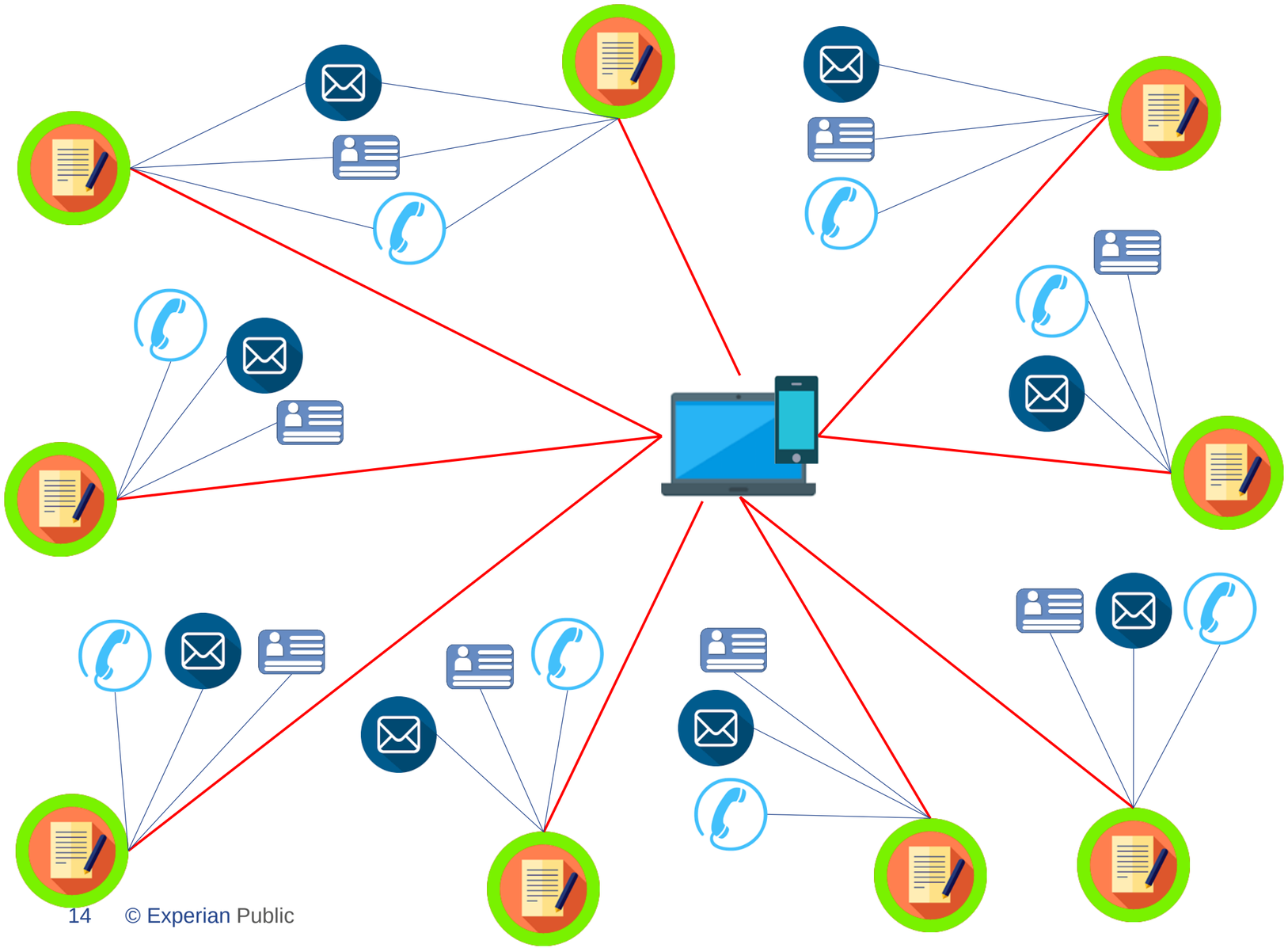
- Paramètres de langue
- Type d’appareil
- Résolution d’écran
- OS
- Version de navigateur
- Fournisseur d’accès
- Heure d’été/hiver
- Nom du plugin Acrobat
- User agent
- Adresse IP
- ID de session

….plus de 160 variables sont collectées en quelques microsecondes

Schéma de traitement du device ID



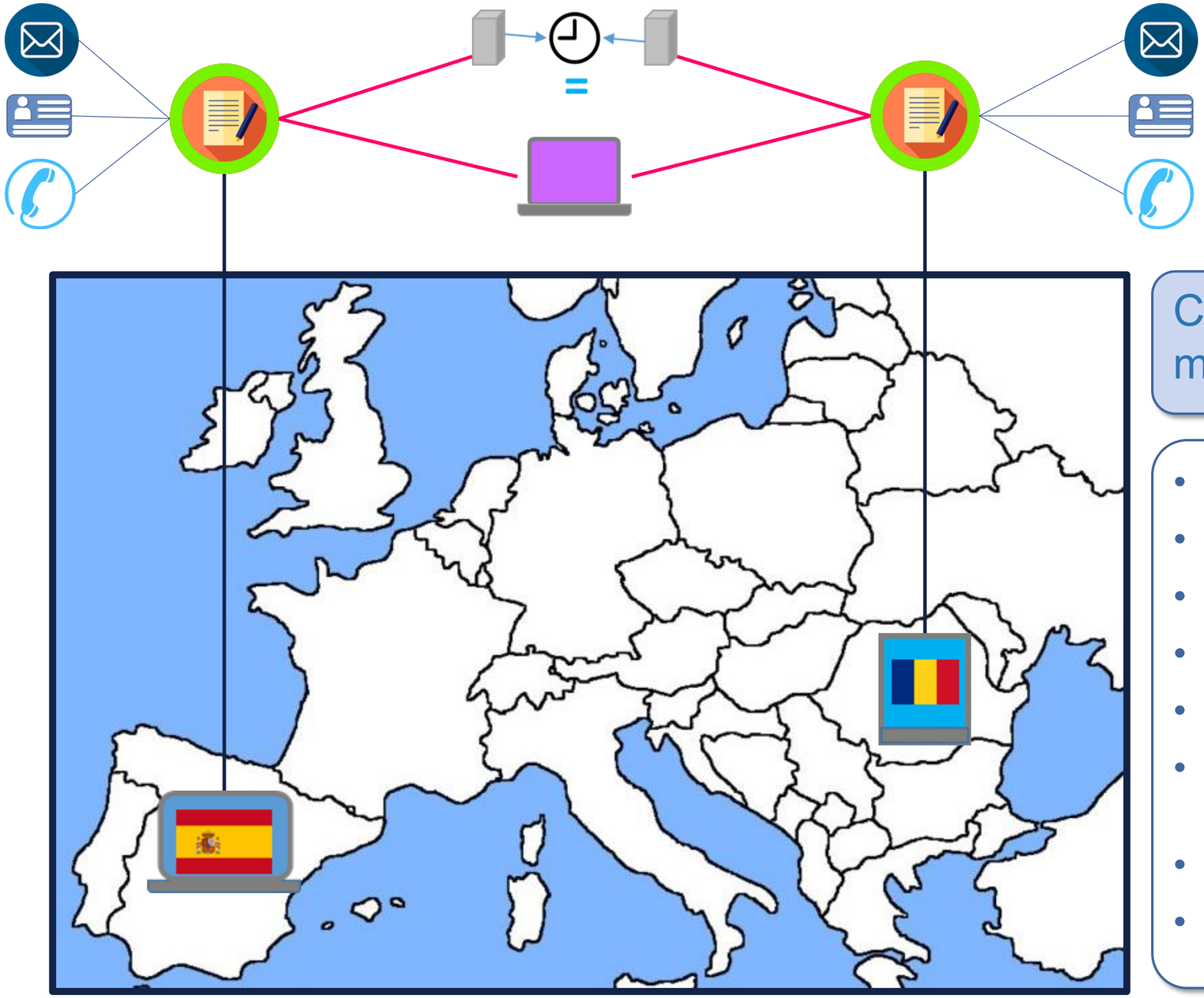
Analyse de liens: cas réels



Cas de demandes multiples avec données client multiples, liées entre elles par un même device

- Le 10 SEP entre 14:46 et 19:54
- 9 demandes **B2C**
- 8 identités différentes
- 8 numéros de mobile différents
- 8 adresses mail différentes
- 8 adresses postales différentes
- 1 seul device
- Montant total demandé: 135 500 €
- Détecté par vélocité sur device

Exemple de prévention d’attaque sophistiquée



Cas d’une demande avec tentative de manipulation de l’origine

- 2 demandes
- 04 SEP 18 entre 14:21 et 14:23
- 2 identités distinctes
- 2 numéros de mobile distincts
- 2 adresses email distinctes
- Première connexion depuis l’Espagne, et seconde depuis la Roumanie
- 2 devices distincts en apparence
- Même TDL et User Agent ➔ même device

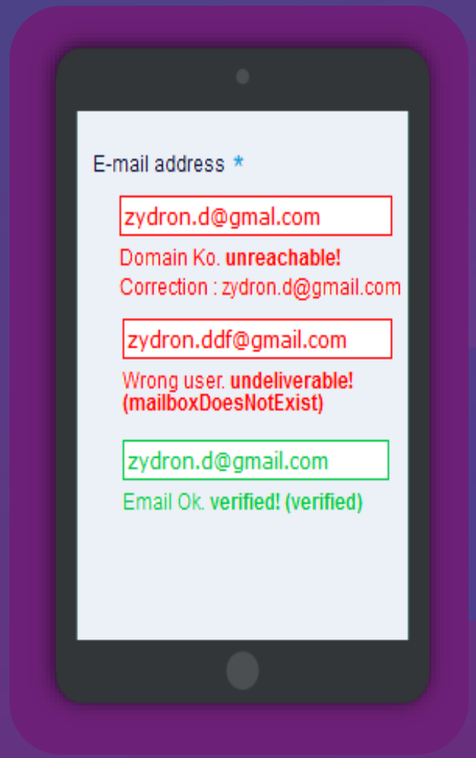
FOCUS TECHNO
“Email Validate”

26/02/2020

Email Validate détails

Vérification fiable de l’adresse email complète

- Solution disponible en **Web Services et Batch**.
- Code retour systématique pour chaque sollicitation :
  - **Verified** : Email vérifié et livrable.
  - **Unreachable** : Domaine invalide (DNS).
  - **Illegitimate** : Email à très grand risque (Spam trap, blackhole, abuse …)
  - **Undeliverable** : Email non livrable (n’existe pas ou pleine)
  - **Disposable** : Email jetable
  - **Unknown** : Manque de précision (Accept all domains, Timeout ...)

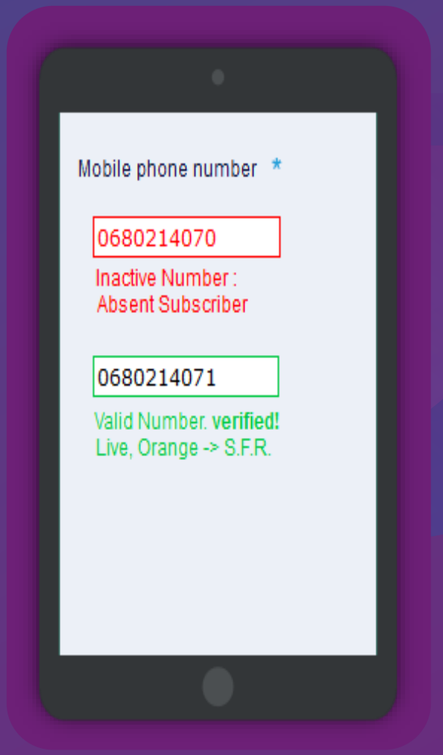


FOCUS TECHNO
“Mobile Validate”

Mobile Validate détails

Vérification en temps réel du numéro de mobile

- Solution disponible en **Web Services et Batch**.
- Base de données centrale pour tous les opérateurs.
- Code retour systématique pour chaque sollicitation :
  - **Absent Subscribers** : numéro désactivé > 1 semaine
  - **Dead** : Numéro non activé ou longue inactivité
  - **Live** : Numéro actif et allumé
  - **No Teleservice Provisioned** : Numéro incompatible avec les appels et messages
  - **Number not supported** : Format non valide (Nb de chiffres, type caractères,…)
  - **Et bien plus …** (roaming, opérateurs, mcc-mnc…)



FOCUS TECHNO
“Vérification documentaire”

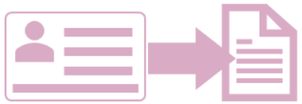
26/02/2020

Vérification documentaire: les 3 grandes fonctionnalités

1

Remplissage automatique de formulaires

Par OCR



2

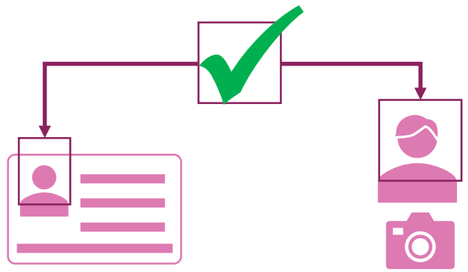
Authentification des documents d’identité

Cohérence bande MRZ avec données

3

Reconnaissance faciale

Par selfie
+ Contrôle de vivacité



FOCUS TECHNO
“Contrôle IBAN”

Contrôle IBAN

- Vérification syntaxique
- Vérification existence
- Détection flambants
- Vérification type de compte
- Vérification cohérence identité

Protocole SEPAmail Diamond

FOCUS TECHNO
“Biométrie comportementale”

Cas d’usage de la biométrie comportementale

Détection des comportements frauduleux (modèles)

Authentification d’utilisateur (reconnaissance du profil de comportement)

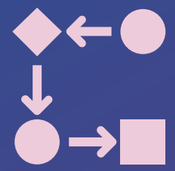
Détection de connexions machines (malware/RAT, robots)

Concepts de base de la technologie

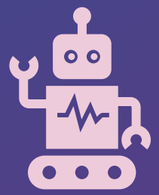
Attributs comportementaux

Caractéristiques cognitives

Modèles d’interaction



Vitesse de frappe



Droitier / gaucher

Copier-Coller vs saisie

Taille de la main

Mode de saisie

Navigation souris / clavier

FOCUS TECHNO
“Machine learning”

Machine learning: optimisation des modèles

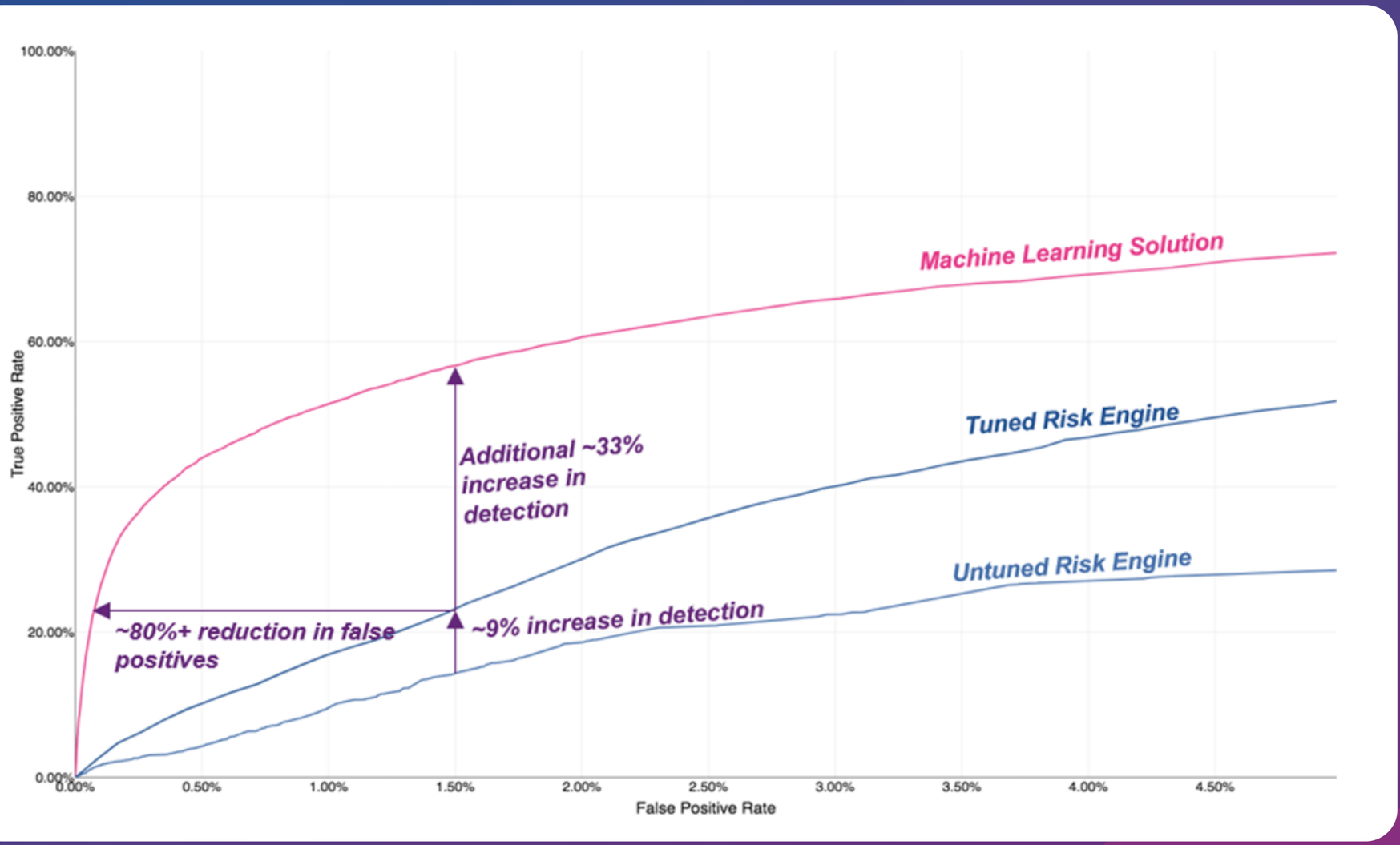
Objectifs:

- **Réduction des faux positifs**
- **Optimisation des détections**
- **Maximisation de l’acceptation**

Moyens:

- **Approche qualitative**
- **Règles « dynamiques »**
- **Granularité maximale**

Machine learning = optimisation des modèles

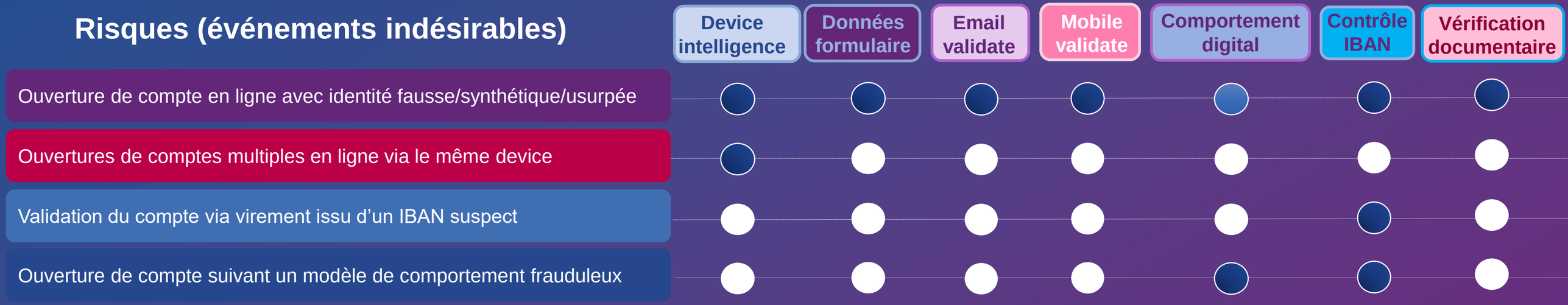


CAS D’USAGE “Ouverture de comptes clients”

Ouverture de comptes clients

Technologies utilisables

Risques (événements indésirables)



Indispensable

Recommandé

N/A

CAS D’USAGE “Protection des comptes clients”

Protection des comptes clients

Technologies utilisables

Risques (événements indésirables)	Device intelligence	Email validate	Mobile validate	Comportement digital	Contrôle IBAN
Accès à de multiples comptes par un même device	●	○	○	○	○
Accès à un même compte par de multiples devices	●	○	○	○	○
Initiation d'une opération par un device non familier du compte	●	○	○	○	○
Update de multiples profils vers une donnée commune (tel, email, …)	●	◐	◐	○	○
Update de profil vers donnée suspecte (Adresse, email, tel,…)	●	◐	◐	○	○
Opérations sur un compte par un utilisateur non familier du compte	○	○	○	●	○
Opérations sur un compte suivant un modèle de comportement frauduleux	○	○	○	●	○
Ajout de nouveau compte bénéficiaire (IBAN) faux ou suspect	●	○	○	◐	●

● Indispensable

◐ Recommandé

○ N/A

Experian et la LCLF

→ Solution dédiée, fondée sur la connaissance du métier de la banque

- Scoring, moteur de règles, ML
- Device Intelligence (technologie propriétaire)

→ Savoir faire global, expertise et implantation locale

Consultants français, issus du métier fraude et du secteur bancaire

Quelques références LCLF
secteur bancaire et financier

BNP PARIBAS PERSONAL FINANCE
UniCredit
Bank of Ireland
SBERBANK
Royal Bank of Scotland
YES BANK
TESCO Bank
citi
РоссельхозБанк
BAYPORT FINANCIAL SERVICES
BANCO DO BRASIL
orange bank
HSBC
BARCLAYS
CRÉDIT AGRICOLE CONSUMER FINANCE
Alfa-Bank
African Bank
HDFC BANK
Santander
mBank
Banco Finandina
Standard Bank