



WEBINAR



Gestion des Alertes LCB-FT

**WEBINAR - RÉGLEMENTATION LCB-FT : NOUVEAUX
DISPOSITIFS ET DERNIÈRES SANCTIONS**

18 Janvier 2022

Sommaire

- Présentation liminaire d'Inetum
- Défaillances de la LCB-FT relevées en 2021 par l'ACPR
- Rappel des mécanismes de génération des alertes LCB-FT
 - Solution standard de filtrage des listes de surveillance de détection
 - Traitement d'une alerte
 - Matrice de décision – Statut de l'alerte
- Approche par la Robotisation
 - Problématique de la gestion des volumes importants de Faux positifs
 - Traitement d'une Alerte/Hit par un RPA
 - Les principes du RPA
 - Quelques métriques
 - Règles de détection en 1^{re} ligne de défense
- Approche par l'Intelligence Artificielle
 - Problématique de la gestion des volumes importants de Faux positifs
 - Approche et étapes du projet du projet
 - Métriques
 - Résultats – Forces et rôle du régulateur
- Conclusions





Présentation d'Inetum

Bonjour!

Votre conférencier et l'offre LCB-FT d'Inetum Consulting

Rôle au sein d'Inetum

Frederic Pace

Manager & practice leader
Conformité & Lutte Anti-Fraude

Spécialisé dans les problématiques de Conformité, Fraude, OnBoarding et KYC. Mon parcours professionnel m'a permis d'aborder les problématiques de **conformité** et réglementation bancaire au travers de missions majeures à la SGCIB comme Responsable du projet de déploiement du Workflow Client OnBoarding puis comme gestionnaire France de l'outil d'entrée en relation pour BNPPARIBAS et enfin comme consultant conseil métier Fraude et Conformité LCB-FT auprès de Personal Finance.

L'offre LCB-FT d'Inetum Consulting

Efficacité opérationnelle et organisation des activités de conformité

- Renforcer le dispositif de la conformité en matière de criblage/filtrage PP/PM, par l'optimisation du **processus KYC**, le scoring des risques.
- Le suivi/pilotage de la gestion des **listes Sanctions/PEP** alimentant les outils de criblage/filtrage et robotique.
- Le suivi et pilotage des analyses puis plan d'action en matière de **Data Quality** des bases clients.
- Evaluer les dispositifs existants par rapport aux préconisations du régulateur, identifier les risques/écarts, proposer les ajustements nécessaires, et suivre leur mise en œuvre.
- Le suivi statistique & KPI de l'outil.
- Le pilotage du dispositif robotique en appui du dispositif humain de traitement des alertes Sanctions/PEP (**TOM**).

Optimisation et rationalisation des activités de criblage / filtrage

- **Robotisation** : identifier / choisir un éditeur « RPA », rédiger les spécifications fonctionnelles pour un RPA Sanction-Pep, aide à la maintenance des RPA Sanction / Pep
- **IA** : Identification des éditeurs, rédaction des fonctionnalités demandées et requises, gestion du déploiement de l'outil, identification des données nécessaires à l'apprentissage, revue des modèles, analyse des résultats.

Reporting et monitoring transactionnel

- Etudes et proposition de **scénarii** comportementaux.
- **Identifier et déployer** des outils de monitoring cibles : fonctionnalités requises, data nécessaires, suivi de projet.

Le Groupe Inetum

Une hybridation d'offres et de compétences spécialisées, avec des expertises sectorielles dédiées et une large couverture géographique



26
Pays

France, Spain, Portugal, Italy, Belgium, Mexico, Luxembourg, Poland, Morocco, Romania, Switzerland, Brazil, Tunisia, Colombia, Cote d'Ivoire, Peru, USA, Angola, Cameroon, Singapore, England, UAE, RP of Panama, Chile, Costa Rica, Dominican Republic, Argentina



27 000
Consultants

Dont 150 dans le Conseil Services Financiers

Conseil en gestion
Conseil aux DSI
Transition ESG
Stratégie des données
Idéation et innovation
Nouveaux modèles opérationnels

Offre efficacité opérationnelle
 Paiement
 Conformité & Fraude



21
Centres de Services

APAC
Brésil
Colombie
France
Inde
Maroc
Pologne
Portugal
Roumanie
Espagne
Tunisie



10
Practices

Banque numérique
Assurance numérique
Commerce de détail numérique
Services publics numériques
Soins de santé en ligne, Industrie 4.0
Villes intelligentes
Télécommunications numériques
Transport numérique
Données intelligentes et intelligence artificielle



7
Secteurs d'activités

Services publics et soins de santé | **28%**
Services financiers | **23%**
Transport, voyages, services | **13%**
Énergie, services publics et produits chimiques | **10%**
Commerce de détail et biens de consommation | **9%**
Industries | **9%**
Télécommunications, médias et technologies | **8%**



6
Activités

Conseil **5%**
Services d'application **35%**
Intégration de systèmes **20%**
Logiciels **10%**
Services d'infrastructure **20%**
Vente à valeur ajoutée **10%**

**Défaillances
de la **LCB-FT**
relevées en
2021 par
l'ACPR**

Inetum Consulting: défaillances de la LCB-FT relevées en 2021 par l'ACPR consulting

Défaillances constatées sur la gestion des Alertes

Défaillances	Causes probables
Alertes trop nombreuses, non traitées ou traitées trop tardivement	Equipes opérationnelles sous-staffées
Délai de transmission à Tracfin	Mise à jour des listes trop peu fréquente
Non détection des pays à risque	Fréquence de filtrage du portefeuille trop élevé
Absence de filtrage des entrées en relation	Utilisation exclusive de « l'exact match » orthographique uniquement sur les noms, prénoms, DoB*, Pays, N° ID....
Connaissance client insuffisante	Seuil « fuzzy match/logique floue » mal déterminé
Traçabilité partielle	Formation insuffisante à la LCB-FT
Qualité de la donnée insuffisante	Paramétrage de la priorisation des risques insuffisant
Faux positifs non traités	Interopérabilité des différents SI (CRM, KYC, Base client,) entre eux absent
Délais de traitement lents	
Défaut de qualité des Déclarations de Soupçon	Pièces justificatives manquantes ou non mise à jour

Sources : ACPR - LCB-FT : Nouvelle sanction ACPR

Rappel des mécanismes de génération des alertes

LCB-FT



Inetum Consulting: schéma fonctionnel des solutions de filtrage des listes de surveillance LCB-FT

Moteur de détection standard: Criblage – Filtrage et Monitoring

Processus

Détection/Criblage

Moteur de détection des personnes

Entrée en relation

Portefeuille/Stock

Noms – Prénoms
 Numéros d'identité nationaux
 Données géographiques
 Date de naissance (DoB)
 Pays de naissance...



Règles de gestion



Liste Sanctions/Embargos MSC / ADSR

Internal Onboarding Sanction List

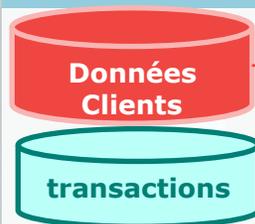
Liste PEP / RCA Adverse Media

Filtrage des transactions

Moteur de détection des transactions

*Le filtrage des transactions vérifie que **la transaction du client n'est pas soumise à sanction internationale** (contrepartie sous sanction) ou à embargo commercial (restriction d'activité pour certains pays).

Pays / Comptes / Client / Devises / Activité / Terroristes listés / Listes sanctions locales



ALERTES BLOQUANTES



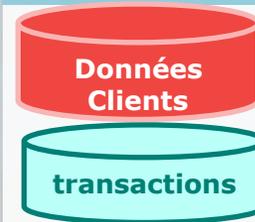
Liste Sanctions/Embargos MSC / ADSR

Monitoring des transactions

Moteur de détection des transactions

** Le monitoring des transactions vise à **identifier des risques de blanchiment ou des transactions anormales en rapport avec les habitudes du client**. Cette surveillance des transactions s'effectue aujourd'hui majoritairement à **posteriori**.

Compte client / comportement / fréquences de retraits / de virements
 Montants / Seuils - Volumes / Seuils - Utilisation de supports
 Pays à risque...Devises

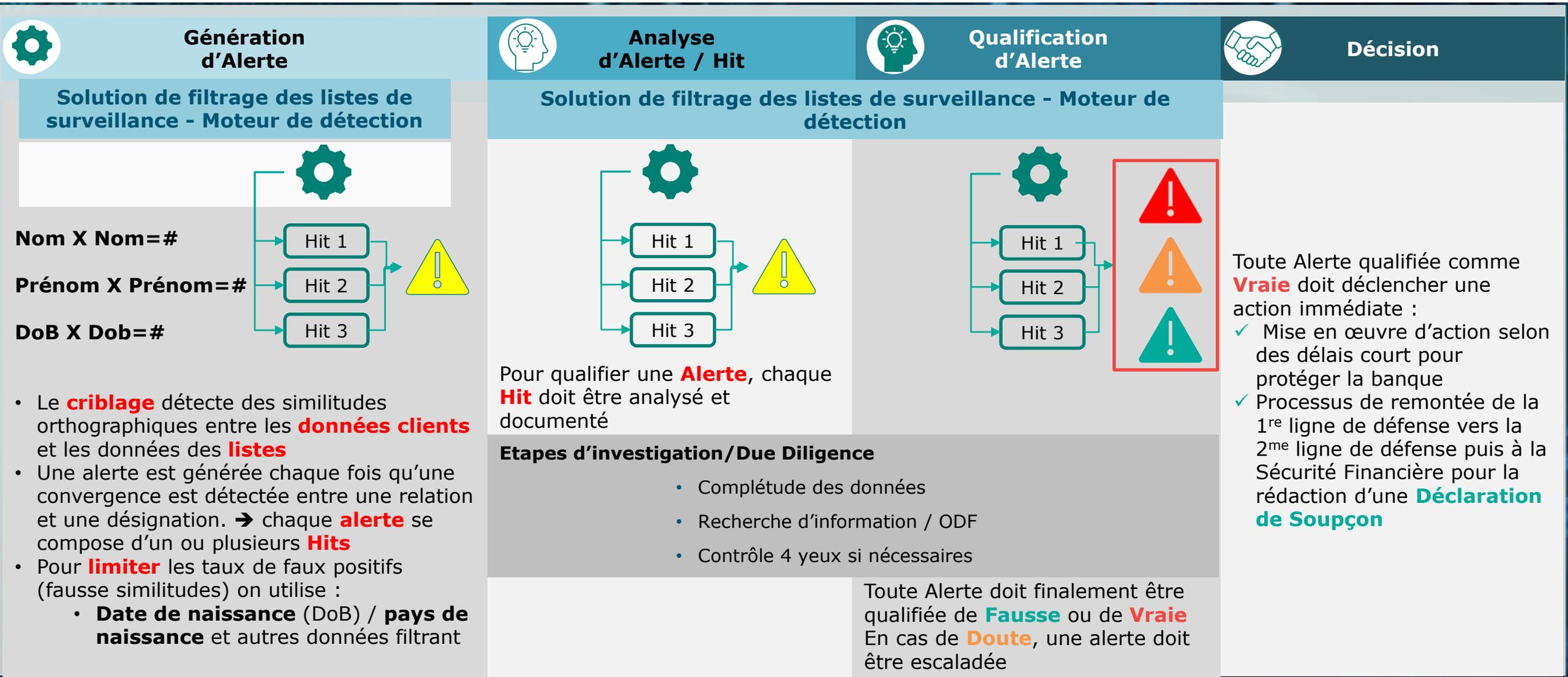


Règles de gestion / Scénari



Inetum Consulting: les principes de gestion d'une alerte

Le traitement d'une Alerte type « Criblage »

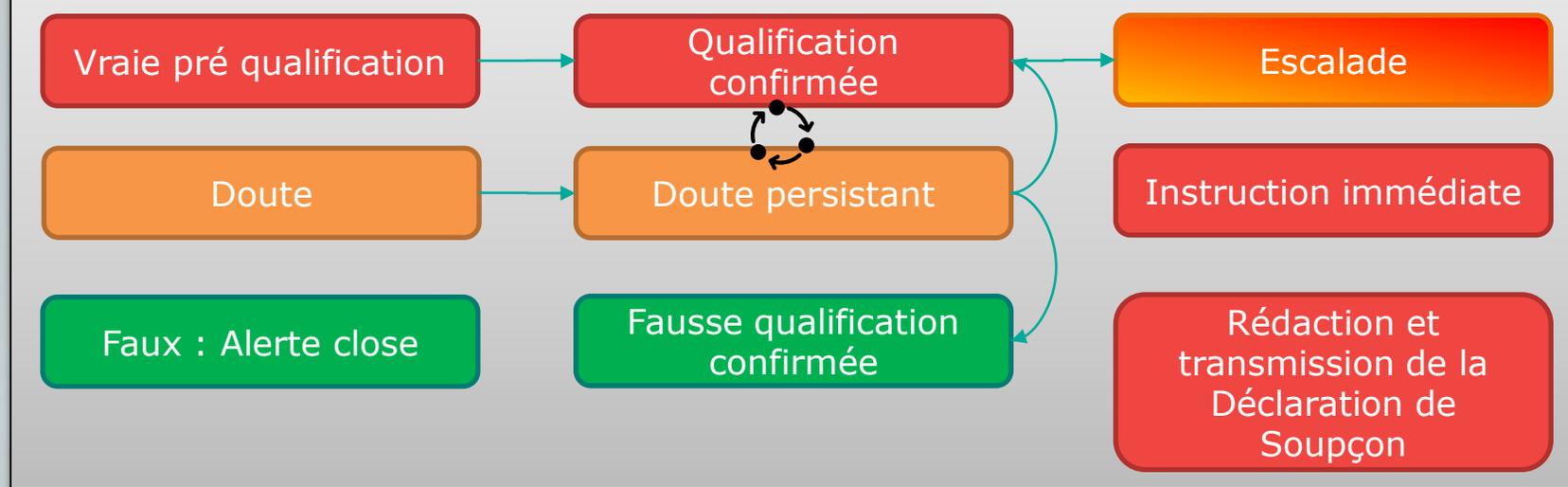


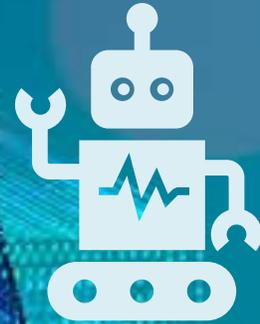
Inetum Consulting: les principes attachés à la gestion des alertes

Matrice de décision d'une Alerte



Statut d'une Alerte-Hit





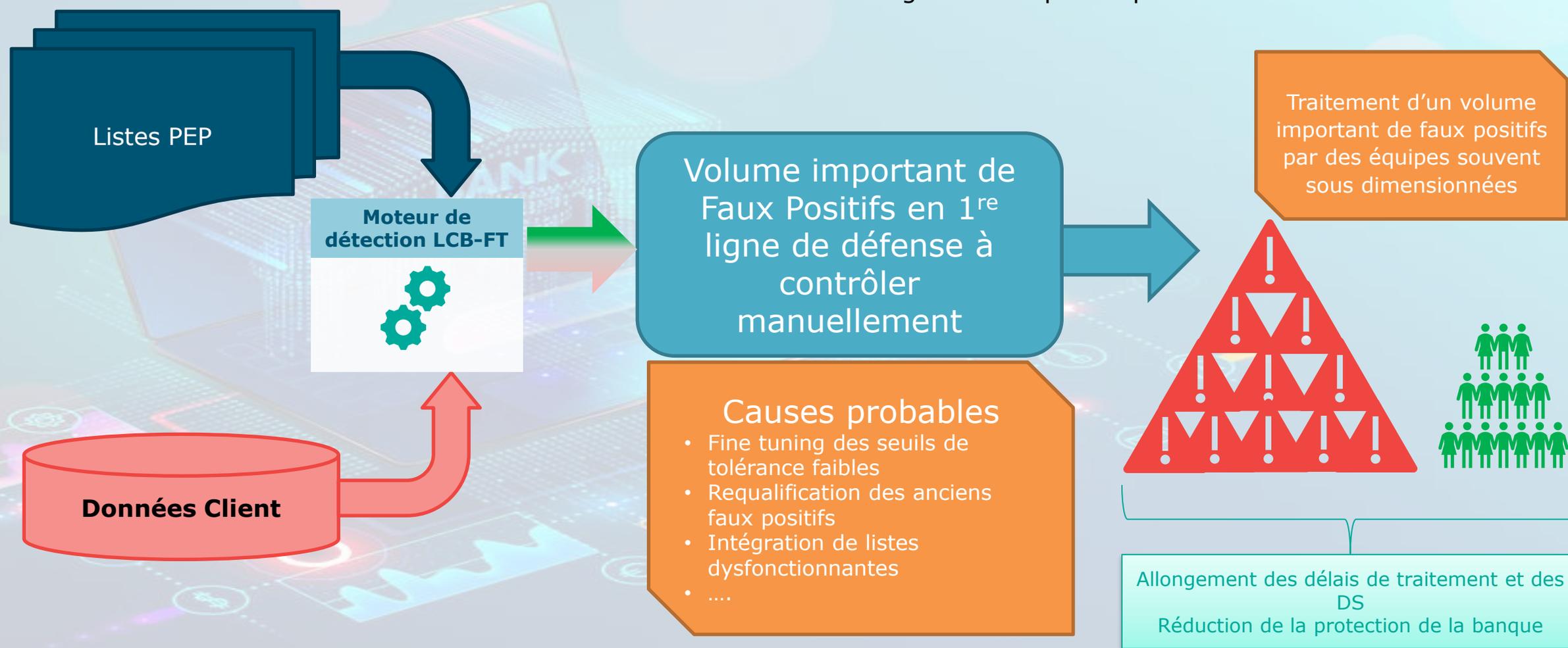
Approche **RPA**

Inetum Consulting: approche RPA

Problématique de la gestion des volumes importants de Faux positifs

Processus criblage

Le principe de précaution devant primer pour protéger la banque, il est préférable d'automatiser le criblage des PEP plutôt que celui des Sanctions



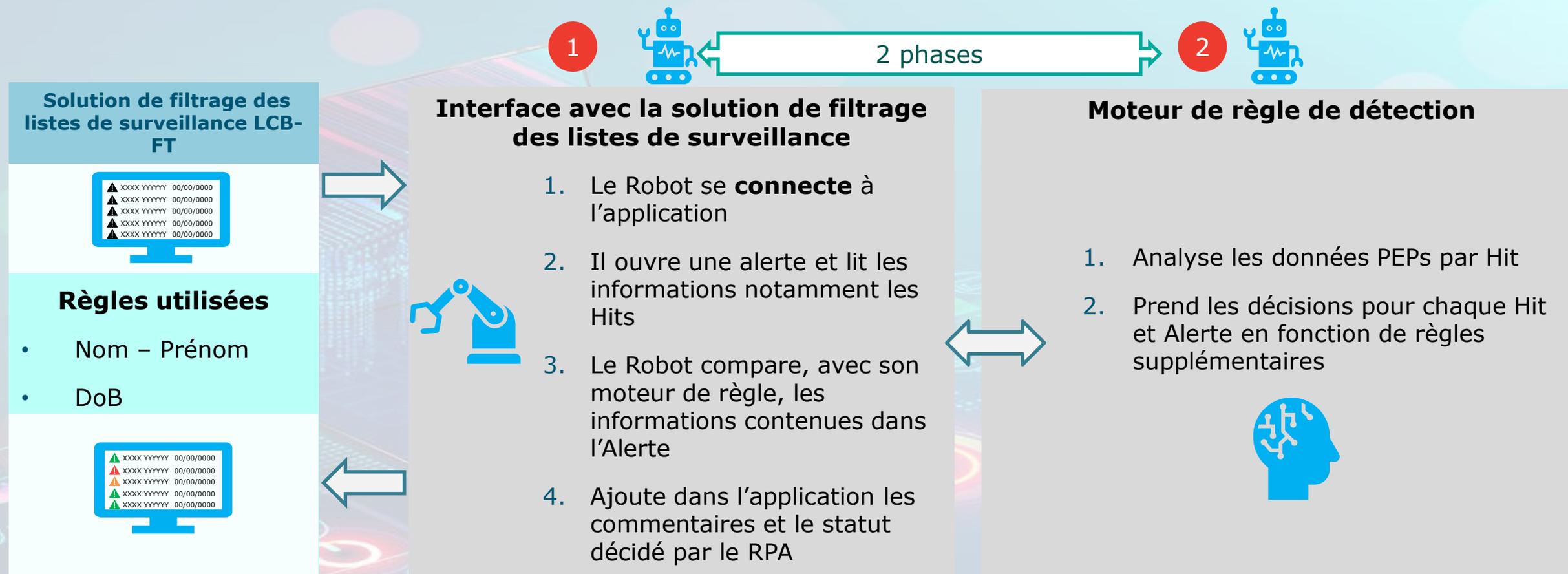
Inetum Consulting: approche RPA

Traitement d'une Alerte/Hit par un RPA



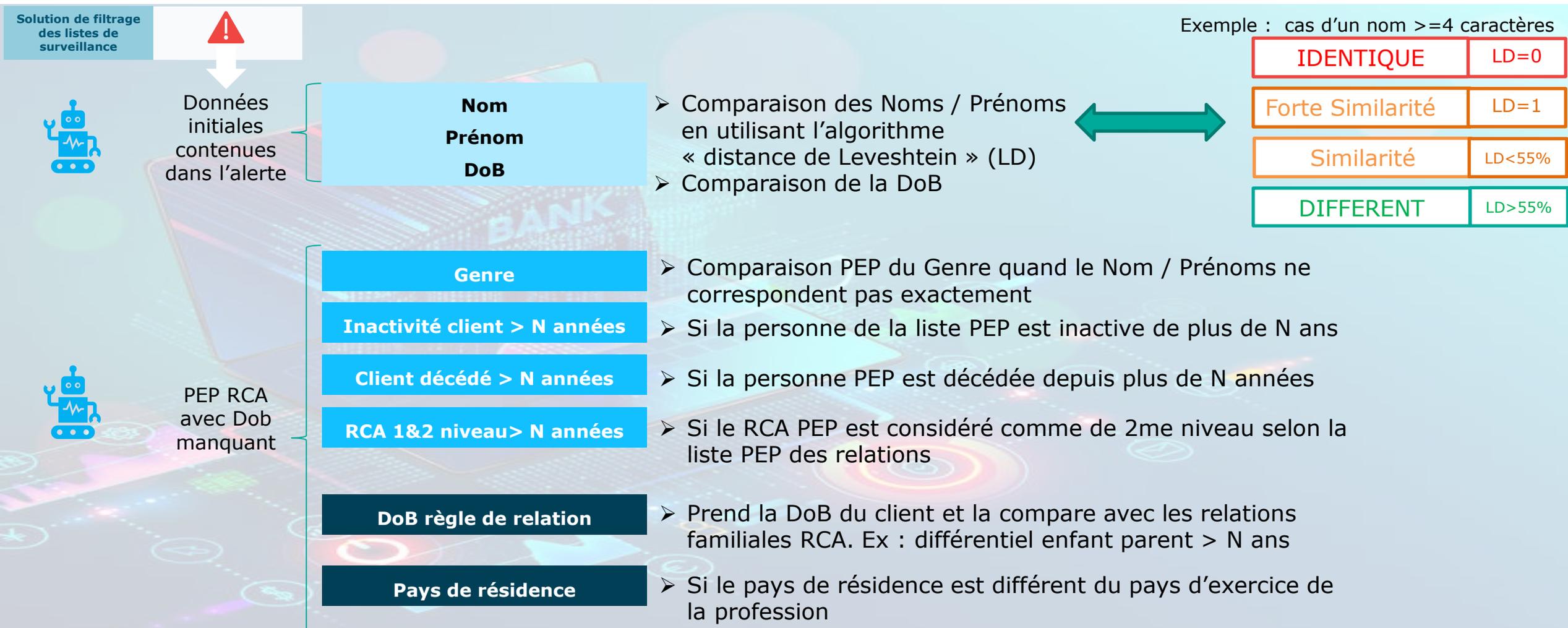
Inetum Consulting: approche RPA

Les principes du RPA



Inetum Consulting: approche RPA

Règles de détection en 1^{re} ligne de défense



Inetum Consulting: approche RPA

Quelques métriques

Le temps de traitement des étapes RPA est **paramétrable**.

Par exemple, en fonction du nombre de données à comparer : la décision du RPA peut prendre **2 minutes**, soit **720** décisions par jour (le RPA travaillant **24/24**) et 22 320 décisions par mois (**30** jours par **mois**).

Ce point de paramétrage est crucial car détermine l'efficacité du RPA.

Le RPA peut être utilisé, par exemple, pour **réduire** un **stock** important d'Alertes/Hits à clôturer tout en permettant à une équipe en 1^{re} ligne de défense ou en 2^{me} ligne de défense de traiter les Alertes du jour.



Approche par l'intelligence Artificielle

Inetum Consulting: approche Intelligence Artificielle

Problématique de la gestion des volumes importants de Faux positifs

Contexte / Besoins

Processus monitoring des transactions

L'utilisation d'outils de monitoring transactionnels basés sur un moteur de règles fait ressortir un nombre **croissant** d'alertes type « **faux positifs** ».

En **2019**, un groupe bancaire a souhaité lancer une étude / **MVP** sur 3 sites différents afin d'intégrer et analyser **les** résultats de l'utilisation d'une solution de type « **Machine learning** » adaptée au **monitoring transactionnel**. L'objectif a été double :

1. Réduire le nombre de **faux positifs**
2. Rendre plus **efficace** le **monitoring** transactionnel

La solution identifiée se base sur une méthode « **non supervisée** » qui vise à identifier les écarts de **comportement** d'un client typique au travers **d'algorithmes pondérés** et **combinés** entre eux sur un mode **d'apprentissage**.

Inetum Consulting: approche Intelligence Artificielle

Approche et étapes du projet du projet

Approche



Identification d'une **Fintech** retenue pour sa solution de **Machine Learning** intégrant les modules de : WF, Reporting, Paramétrage, Interface analytique et Rule Based.



Test sur **12 mois** : « Parallel Run » entre une solution de monitoring transactionnel classique et l'IA. Objectif → s'assurer que l'outil d'IA génère les **même nombre d'alertes** et **Déclaration de Soupçons** que la solution classique.



L'outil embarque des algorithmes permettant **l'auto apprentissage** du comportement.



Volume du MVP : **35 Millions** de **transactions** avec **18 mois d'historique** pour **1 million** de **clients**



Mobilisation des équipes projets et métiers : équipes 1^{re} ligne de défense + 2^{me} ligne de défense (6 max), data-scientist internes (2) et Editeur (2)

Etapes

Extraction des données :

- Autorisation d'extraire des données à caractère personnel à partir de la base des Alertes et du SI transactionnel avec Obligation de maintenir les données dans des serveurs locaux
- Autorisation d'utiliser les composants standards propres à l'IT du client



Fiabilisation des données

- Intégrité (latin ou cyrillique?), duplication, données absentes... (4 mois)



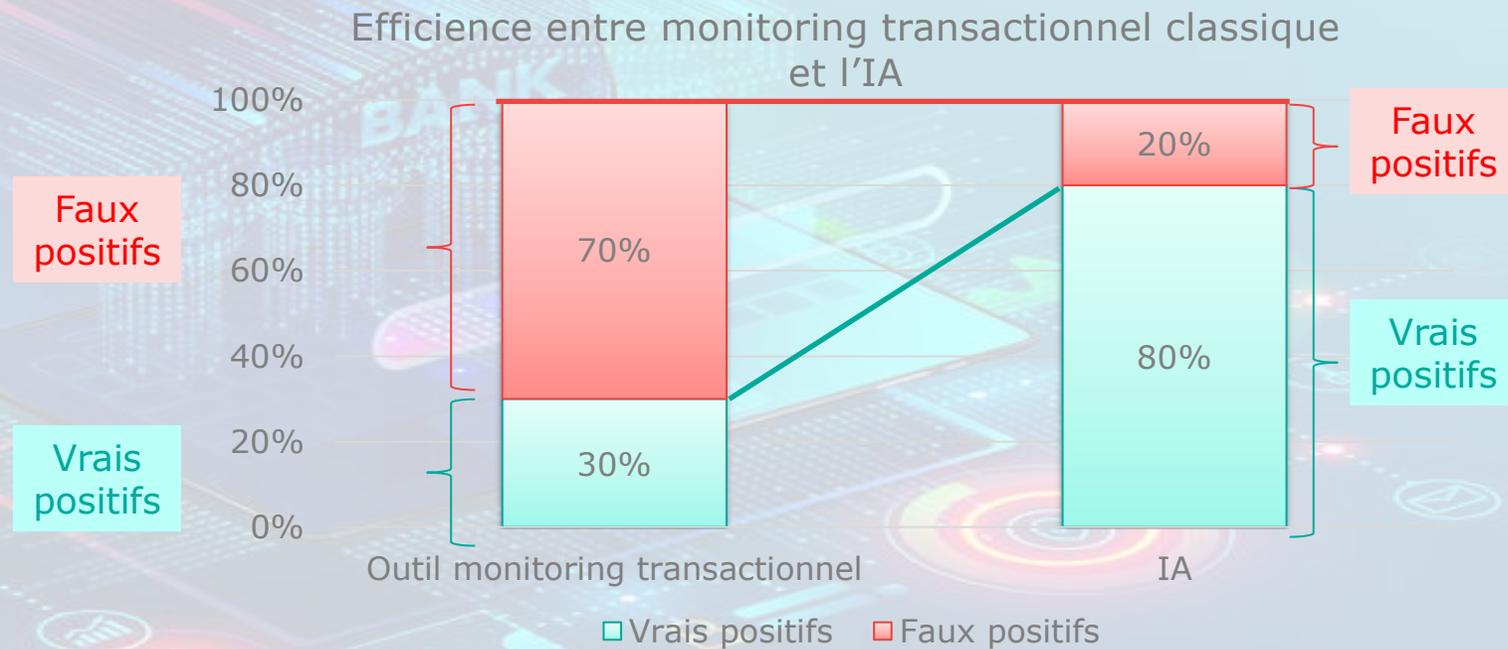
Apprentissage itératif

- Correction, erreurs, combinaison des algorithmes, analyse approfondie des alertes et tester le modèle avec données jamais vues auparavant

Inetum Consulting: approche Intelligence Artificielle

Métriques

Résultats en chiffres



Inetum Consulting: approche Intelligence Artificielle

Résultats – Forces et rôle du régulateur

Résultats issus des 3 « parallel RUN » : Intelligence Artificielle vs outil de détection classique

 Capacité à **augmenter** significativement le nombre d'alerte **pertinente** (Vrais positifs) → **80%** vs 20 à **30%** pour l'outil de détection classique



Détection des même **SAR**

 Identification de **nouveaux** cas **suspicieux** non détectés par l'outil de détection classique avec une capacité à **détecter plus** de cas sophistiqués

→ Le double Run ne permet pas de **réduire** le nombre d'**Etp** directement

→ A terme (lors de l'autorisation d'utiliser l'IA à 100%) il y aura un impact sur le **TOM** : des **transferts** de compétences et d'expertises sont à prévoir entre la **1^{re} ligne de défense** et la **2^{me} ligne de défense**.

 L'interface ergonomique de l'outil a sensiblement facilité le travail d'analyse → **30%** de gains efficient prouvés

Forces et paradoxe avec le régulateur

 **Des situations inattendues non couvertes par les scénarii classiques:** l'approche multidimensionnelle sans seuils permet d'élargir le périmètre d'analyse qui n'était pas auparavant imaginé et mis en place par les experts.

→ Un système basé sur des règles limite la détection au risque

Le régulateur (**ACPR**) souhaite maîtriser l'IA des banques :

- Création du pôle Fintech-Innovation et du programme SupTech
- Pose les principes de la supervision de l'IA
- Accompagne l'écosystème par des séminaires et pratiques
- Propose une boîte à outil d'audit de l'IA



Conclusions

Inetum Consulting: conclusion

La délégation au travers des RPA et de l'IA

AVANTAGES

RPA

// Opérationnel 24/24 & 7/7

Haute disponibilité de la force virtuelle, en fonction de la planification de l'exécution des robot utile en cas de « Mass closing ».

// Rapidité d'exécution

En fonction de la complexité du processus à automatiser, réduction du temps d'exécution pouvant aller jusqu'à 80%.

// Valorisation du travail

Les opérationnels sont réaffectés à des tâches à plus haute valeur ajoutée.

// Contrôle interne

Toute l'activité des automates est tracée via une Piste d'Audit (cf. stockée sur l'orchestrateur).

Intelligence Artificielle

- // Capacité à augmenter significativement le nombre d'alerte pertinente (Vrais positifs) 80%.
- // Réduction de 30% - 50% du nombre d'alerte.
- // Des transferts de compétences et d'expertises sont à prévoir entre la 1^{re} ligne de défense et la 2^{me} ligne de défense.

INCONVÉNIENTS

RPA :

// Maintenance

Nécessite une maintenance quotidienne de 3 à 5 AMOA/MOE.

// Fine tuning

Nécessité de suivre et faire évoluer le fine tuning.

// Plutôt PEP que Sanctions

Il n'est pas encore recommandé de les utiliser pour les alertes Sanctions.

Intelligence Artificielle,

- // Gros consommateur de données historiques.
- // Contrairement aux RPA, elles ont des interférences très fortes avec les systèmes d'information en place.
- // Demande un suivi par une équipe de Data Analyst et Data Scientist.
- // Infrastructure de serveurs supplémentaire.
- // A ce jour, le régulateur préférera un double contrôle par 2 systèmes différents.



Frédéric Pace

Inetum Consulting

Manager & On Boarding, Compliance, Fraud Practice Leader

Cell. : +33 (0)6 47 59 35 89 La Porte du Parc - 145 boulevard Victor Hugo -

93400 Saint-Ouen Tel. : +33 (0)1 44 04 55 95 – Fax. : +33 (0)1 44 04 59 47

frederic.pace@inetum.com



inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE



Inetum : nos références conformité

Nos références 2021

Mission d'efficacité opérationnelle du **criblage des listes sanctions** et **PEP** pour le compte de la conformité centrale

Mission de pilotage de l'intégration et de l'activité de criblage des **Robots PEP**

Mission de Digitalisation des entrées en relation clients – refonte des processus métiers

Mission, côté métier, de suivi de l'intégration d'une solution **d'Intelligence Artificielle** pour l'activité LCB-FT (sous forme de MVP)

Mission d'aide à la définition des scénarii par pays des **règles de détections** LCB-FT

Mission d'étude choix d'un outil (moteur de règle) de détection transactionnelle LCB-FT

Mission d'aide à l'intégration du processus de droit à l'oubli

Clients



L'Expertise **métier** & **fonctionnelle**

Communauté d'experts LCB-FT et Fraude

ASSOCIATION EUROPE FINANCES RÉGULATIONS

Partenariat OCR et Authentification digitale

Une **veille** métier et technologique

Solution Inetum AML – FT & Fraude