Vision d'IBM sur la Lutte anti-fraude

Oleg Ivanov – Architecte logiciel
Banking Industry

La lutte contre la fraude est devenue un enjeu majeur pour les entreprises

- **46% des entreprises françaises** sont victimes de la fraude

- Les entreprises renforcent les moyens de lutte contre la fraude dans un **contexte économique difficile**

- Les responsables privilégient le choix de solutions de lutte anti-fraude qui **offrent un ROI rapide**

- Ce que disent nos client:
  - Les activités frauduleuses continuent de progresser
  - Les fraudes organisées, en réseau, se répandent
  - Une inquiétude croissante concernant le e-commerce
  - La fraude interne demeure prépondérante
  - Il n'y a pas assez de ressources pour traiter l'ensemble des fraudes

"Détournements d'actifs, fraudes comptables, corruption, cybercriminalité, un tiers des entreprises dans le monde sont victimes de fraude. En France, la fraude touche près d'une entreprise sur deux."

*Source: PWC, "**Global Economic Crime Survey 2011**"*

Détecter et investiguer la Fraude est devenu de plus en plus abordable

On dispose d'une marée d'informations à analyser…

Volume de données

Variété de l'information

Vitesse de décision

Source: IBM Institute for Business Value

Besoin de visibilité

Nécessité de prédire

Données analysées dans un contexte

"…40 exabytes de données créées en 2008…
Plus que durant les 5,000 dernières années…"

Les principales actions de lutte contre la fraude engagées par nos clients

Dissuasion → Prévention → Détection → Investigation → Recouvrement

Processus d'amélioration continue

Pilotage de la lutte contre la fraude

Cartographier la fraude et en évaluer les enjeux	Partager les informations entre administrations/établissements	Assurer le suivi de l'activité
Fixer les priorités & aligner les ressources	Disposer des « bonnes » informations sur les personnes	Anticiper les « nouvelles » formes de fraude et définir les règles de traitement

La détection proactive et réactive

Détection proactive : modéliser la connaissance pour identifier des clignotants



Commission des faits

Les différentes techniques utilisées

Méthode dirigée :

Création d'un modèle prédictif à partir d'une base de Fraudes Avérées :

- **Il est possible de construire un modèle statistique capable d'identifier les variables expliquant la fraude**

- **Si on dispose d'un faible nombre de fraudes, on peut recourir en utilisant :**
  - Des techniques d'échantillonnage disponibles dans IBM® SPSS® Modeler
  - De méthodes d'arbre de décision afin de valider les règles avec l'aide d'experts métier

- **Il est nécessaire de suivre très régulièrement les modèles afin de les adapter aux nouveaux comportements de fraude**

Méthode non dirigée :

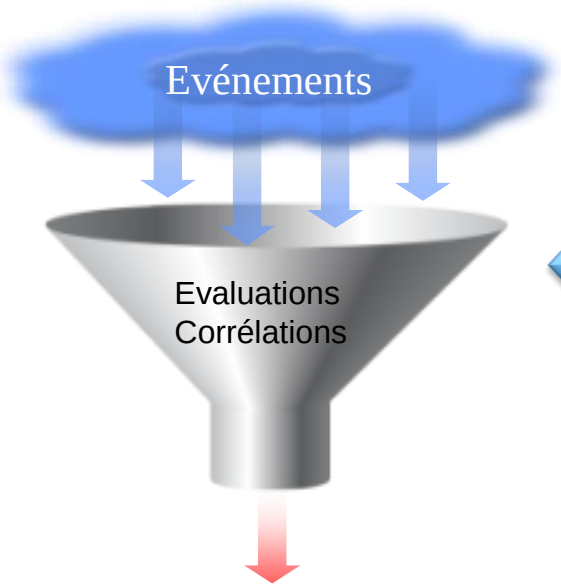
- **On utilise des techniques de détection d'anomalies ou de déviation par rapport à la norme pour identifier des cas de fraude suspects et potentiels**
  - Notre solution dispose de fonctions pour trouver des comportements atypiques
  - Enrichissement continu de la base de fraudes avérées

Méthode basée sur des règles métiers :

- **Implémentation de systèmes de détection à partir des règles métiers issues de cas avérés**

Les techniques de lutte contre la fraude
Couplage « prédictif » et « moteurs de règles »

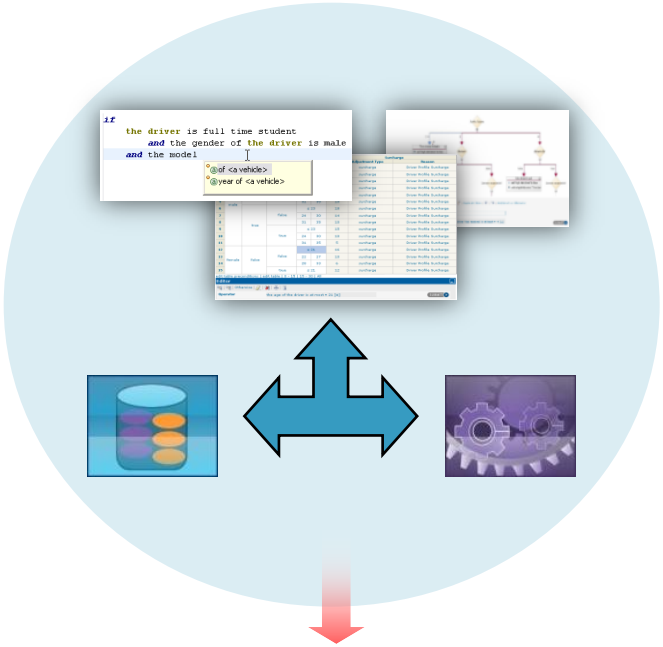
Prédiction



Détection / Scoring

- Détecte quand les événements ou patterns se produisent et notifie les acteurs ou systèmes pour action

Prescription



Décisions / Actions

- Prescrit l'action appropriée grâce à l'exécution de règles métier, en fonction du résultat calculé en amont

Les techniques de lutte contre la fraude

S'intéresser à l'identité

Sources Entreprise & Externes

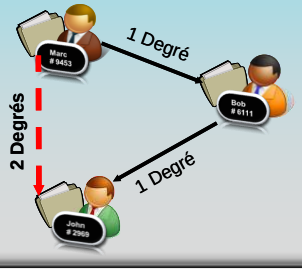
Web Service permettant l'intégration des processus métier

Qui est qui?

- Etablir une identité unique
- Attributs physiques et digitaux
- Personnes et Organisations
- Noms multiculturels

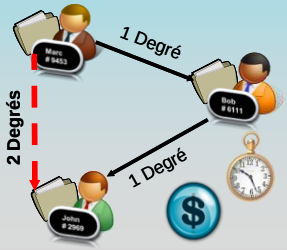
Qui connaît qui?

- Lien évident et non évident
- Lien entre les gens et les groupes
- Degrés de séparation
- Rôle d'alertes



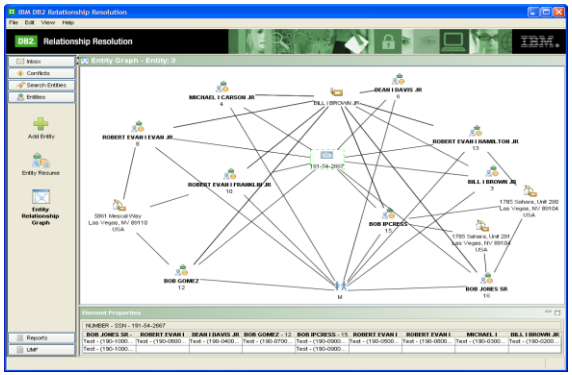
Qui fait quoi?

- Événements et transactions
- Processus d'événements
- Critères d'alerte
- Quantifier les activités liées à l''identité



Alerte

Chaque nouveau candidat est comparé instantanément à d'autres entités et à des données historisées

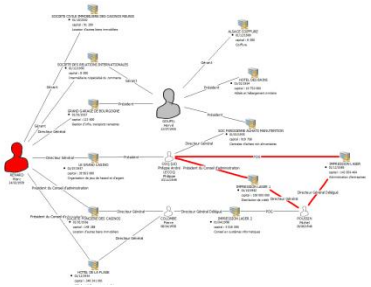


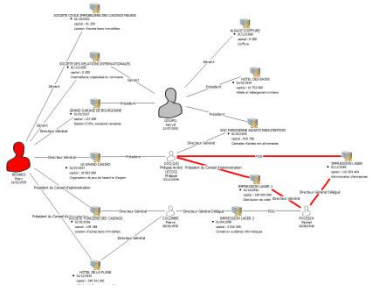
Principales fonctionnalités

- **Résolution :**
  - **Résolution d'identité (Qui est qui)**
  - **Résolution de relation (Qui connaît qui)**
  - **Gestion des activités (Qui fait quoi)**
- **Règles de composition et de corrélation facilement personnalisables**
- **Correspondance floue - Identité claire**
- **Self Healing / Auto Correction**
- **Peut fonctionner en mode batch et en temps réel**
  - **Mise à jour des identités au fil de l'eau**
- **Capacité à rapidement traiter une masse importante de données**
  - **Prise en charge de sources de données illimitées**

La détection proactive et réactive

Détection réactive : modéliser le comportement humain pour identifier des actes



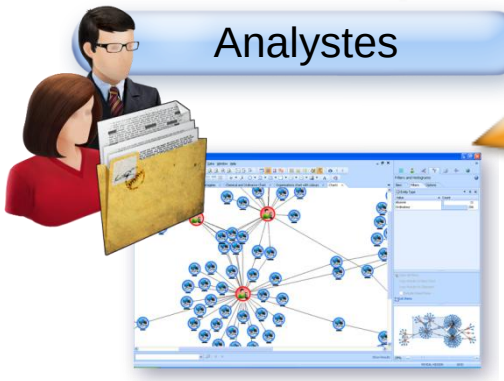


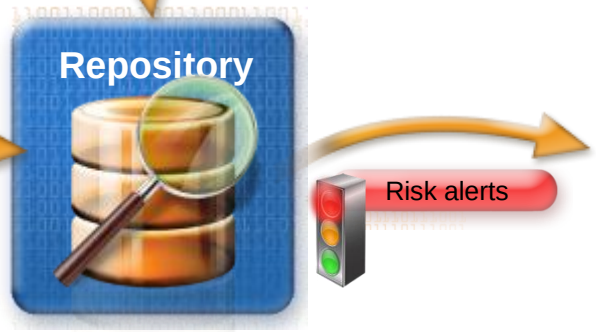
Commission des faits

Les techniques de lutte contre la fraude

L'investigation des alertes

Fusionner les informations structurées ou non pour enrichir l'analyse





Appréhender toutes les facettes d'un réseau dans un environnement d'analyse unique

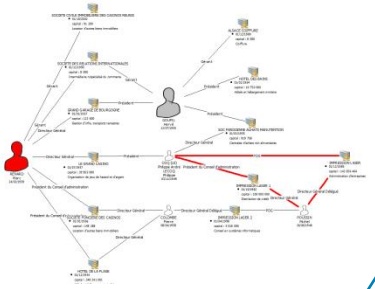
Executive view for Risk, Compliance and Security

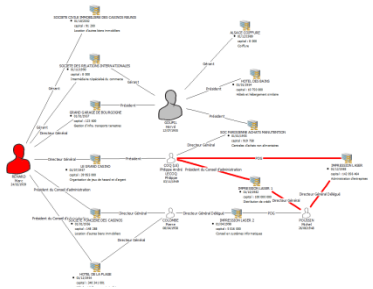
Internal Investigation Unit

External partners

La détection proactive et réactive

Détection réussie et efficace : les deux simultanément





Commission des faits

Solution IBM de gestion de la Fraude – Fonctionnalités

SANTE-SOCIAL | FISCAL | DOUANES | SECURITE DU TERRITOIRE | ASSURANCE | BANCAIRE | DISTRIBUTION

Real-time

Discovery

Identité

Listes de surveillance

Combines

Risque

Detection

Modèles prédictifs

Règles

Patterns

Decision Management

Management

Création de cas & Workflow

Analyse de contenu

Optimisation des analyses

Investigation & Remediation

Gestion des cas

Analyse de liens cachés

Investigation

Reporting

Reporting opérationnel

Tableaux de bord

Feedback

Information Domains

Sources Internes

Sources Externes

Contenu non structuré

Bases de fraudes avérées

Solution anti-fraude pour l'octroi de crédit – Architecture fonctionnelle