Lutter *(efficacement)* contre les fraudes, l'impérieuse nécessité d'innover

François JAUSSAUD, fjaussaud@orusadvisors.com
Paris, le 18 septembre 2013

Le Groupe Keyword

1985

L'année de naissance du Groupe Keyword.

Le Groupe Keyword est une entreprise française – pas d'off-shore.

2

Aujourd'hui, le Groupe Keyword développe deux activités:

- Un cabinet de conseil : Orus Advisors (Paris) ;
- Un Editeur-Intégrateur : Keyword (Montpellier).

+50%

C'est la croissance du chiffre d'affaires de Keyword sur l'année fiscale 2012 – 2013 (clôturée en juin 2013).

2004

Orus Advisors, le porteur de la vision métier : une expertise sur les sujets de lutte contre le blanchiment et les fraudes développée depuis 2004 chez IBM GBS puis au sein du Groupe Keyword.

2006

Naissance du partenariat avec IBM sur la base de technologies partagées : Java/J2EE. Aujourd'hui, Keyword est en passe de rejoindre le petit groupe des « IBM Business Partner Premier ».

>10 Millions d'euros

Keyword, le porteur de la technologie, éditeur des progiciels métiers ISIMAN ; les équipes Solutions et R&D conçoivent les solutions et les déploient depuis 28 ans.

- A ce jour, les investissements faits en recherche & développement sur la plateforme ISIMAN représentent plusieurs millions d'euros depuis 1999 … et les investissements continuent.

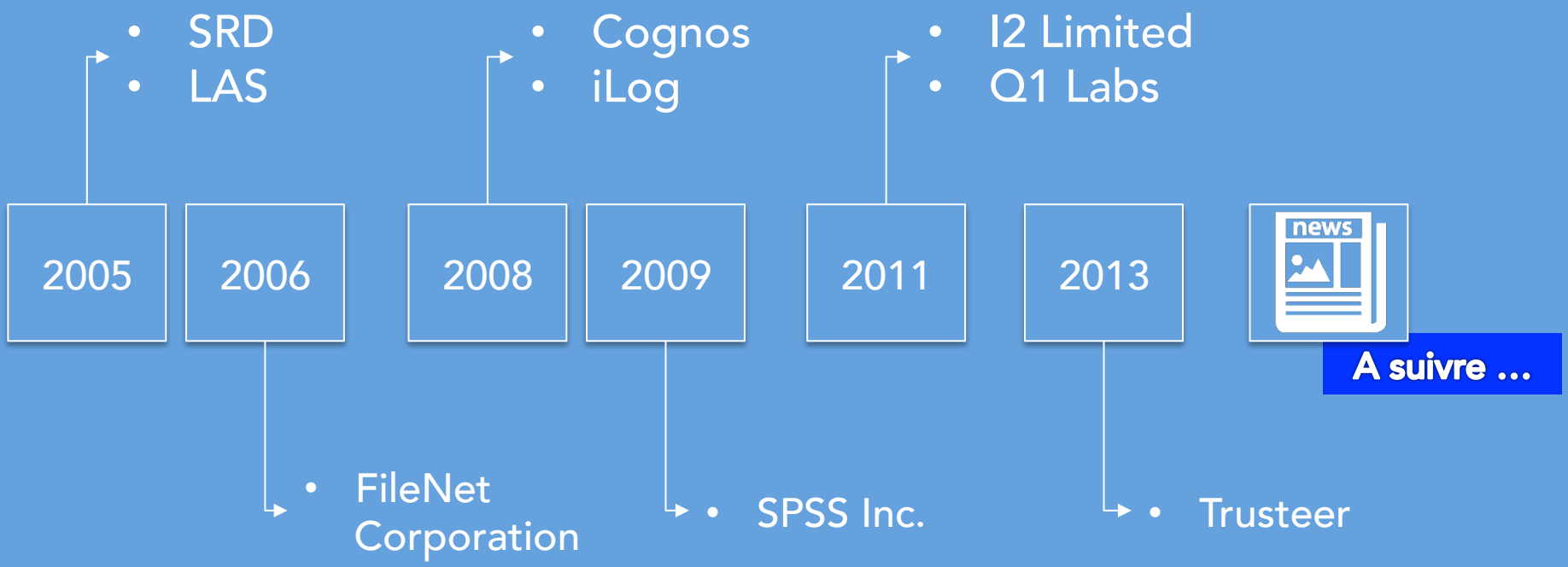
IBM et la lutte contre les fraudes : Un chiffre

USD +14.000.000.000

14 milliards de dollars, c'est une estimation (grossière et probablement inférieure à la réalité) du coût des acquisitions d'éditeurs de logiciels réalisées par IBM dont les technologies présentent un intérêt direct pour lutter contre les fraudes ...

… et ce n'est pas fini !

IBM et la lutte contre les fraudes : IBM acquiert régulièrement des technologies, les pérennise et poursuit leur développement.



IBM + Keyword : une solution packagée et sur-mesure

Face à un problème aussi complexe et exigeant que la lutte contre les fraudes, IBM a choisi de travailler avec le Groupe Keyword pour apporter à leurs clients communs une solution packagée et sur-mesure.

Une ambition affichée d'IBM et Keyword : être considérés comme des partenaires d'innovation, des créateurs de valeur pour les établissements financiers.

Les origines de l'impérieuse nécessité d'innover : tous les secteurs d'activité sont touchés par la fraude interne et la fraude externe.

« Plus de 2 milliards d'euros disparaissent annuellement dans les **fraudes à l'assurance**. Un coût qui se répercute sur le montant des cotisations. En assurance auto, on constate surtout des fraudes à la déclaration et des fraudes au sinistre. »

« **Arnaque à la mutuelle** : des lunettes de soleil à l'œil - Une enquête vient d'être relancée à Marseille : des opticiens sont suspectés d'avoir arnaqué la mutuelle de la RTM. »

« **Deux dentistes** (…) facturaient un montant 28 fois plus élevé que la moyenne départementale (13) pour une couronne, déclaraient recevoir en moyenne 70 patients par jour et multipliaient les actes au point que cela représentait 52 heures de travail quotidien ! Le jeune dentiste de 32 ans et son père qui travaillait à mi-temps réalisaient ainsi un chiffre d'affaires annuel de 1 à 1,2 million d'euros. »

« **Fraude fiscale** - Les estimations donnent le vertige : 60 à 80 milliards d'euros rien que pour la France. »

« **Fraude à la carte bancaire** : L'Observatoire de la sécurité des moyens de paiement de la Banque de France a en effet constaté en 2012 une augmentation significative de la fraude au niveau international (+11,2 %) due à une recrudescence des vols de cartes et du piratage de données. »

« Vaste **escroquerie aux virements bancaires** en Rhône-Alpes : Une escroquerie a touché une douzaine d'entreprises autour de Lyon, St-Etienne mais aussi Clermont-Ferrand, selon le Progrès. Il s'agit pour les malfrats d'obtenir de ces sociétés le virement d'une grosse somme d'argent. Depuis deux ans, le montant du préjudice dépasserait les 20 millions d'euros. »

« La principale affaire à laquelle JP Morgan est confrontée est sans doute celle de la "**Baleine de Londres**" qui n'en finit pas de rebondir. Deux anciens employés, dont un Français, Julien Grout, pourraient ainsi être poursuivis aux Etats-Unis. Cette affaire, qui fait suite aux prises de position d'un trader français Bruno Iksil, a déjà coûté 6,2 milliards de dollars à l'entreprise américaine. »

« **PIRATAGE MASSIF DE CARTES BANCAIRES** – USA : CARREFOUR ET DEXIA PRIS DANS LE PIÈGE : 5 pirates d'Europe de l'Est sont inculpés dans l'un des plus grands dossiers de cybercriminalité des Etats-Unis. La fraude s'élève à 300 millions de dollars. Sur le volet européen, Carrefour et Dexia sont touchés. »

« **Faux permis de conduire** : L'an passé, 14.500 titres ont été soumis à la BFD. «En général, on compte 10 à 15 % de faux», signale Frank Willems. Mais le taux peut être plus élevé : en Ile-de-France, sur les 1789 permis suspects, 367 se sont révélés être des imitations. Le plus souvent, il s'agit de titres étrangers. »

Les origines de l'impérieuse nécessité d'innover : accélération, amplification, banalisation et professionnalisation ?

- Les fraudeurs sont perpétuellement en mouvement ; ce n'est pas nouveau.

- Ce qui est nouveau, c'est :
  - L'ampleur et l'accélération du phénomène ;
  - La grande mobilité de bandes organisées (mafias) capables de mener des actions commandos ;
  - La tentation de « Monsieur Tout-le-monde » de frauder pour arrondir ses fins de mois
    - Un vrai problème culturel : « Frauder c'est voler ? Ah … Je ne savais pas ! » ;
    - L'accès « grand public » à des techniques et outils pour frauder via internet ;
    - L'industrialisation des « packs URSSAF » et des faux documents chaque jour plus « bluffant ».
  - La police et justice sont encombrées et les établissements ne portent pas plainte pour dénoncer les tentatives ; un étrange sentiment d'impunité se développe et crée un phénomène d'entrainement particulièrement redoutable.

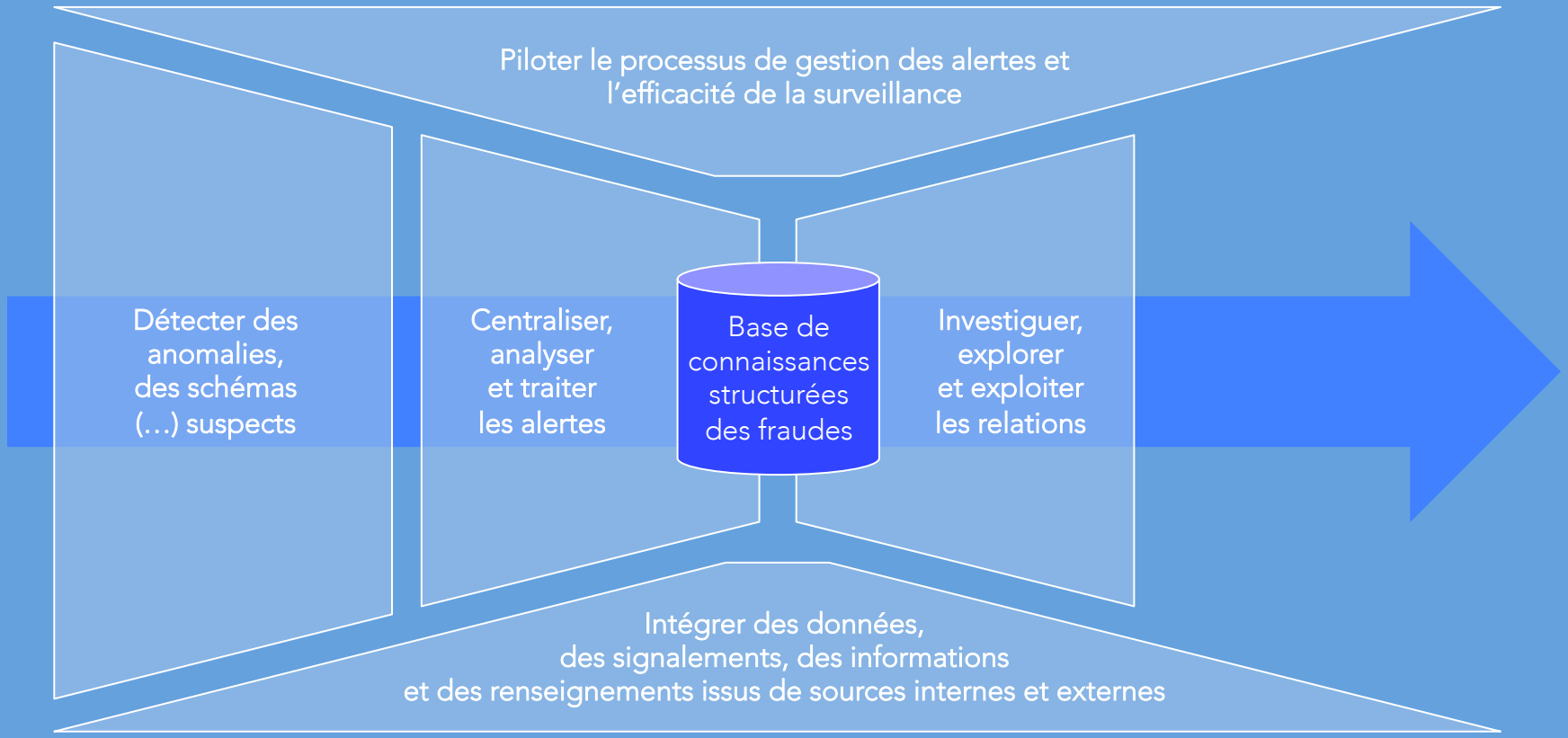
- Le coût estimé de la fraude : entre 5% et 7% du PIB (pour les pays industrialisés).
- Une simple fraude « documentaire » couterait en moyenne 10.000 euros à une banque de détail.

Deux clefs pour lutter efficacement contre les fraudes : 1) combiner les analyses déductives et inductives

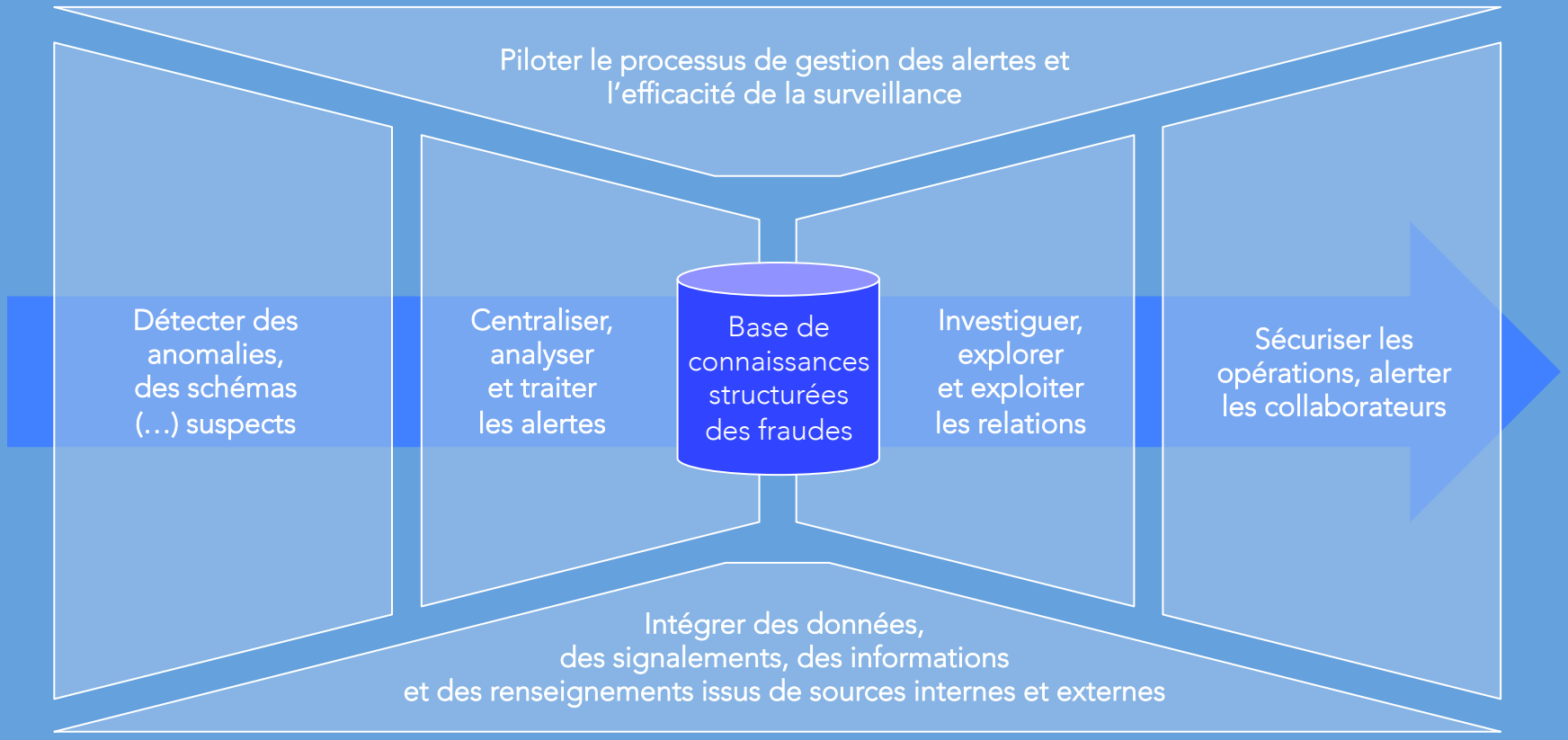
Déduction : de la donnée à l'information

Induction : de l'information au renseignement

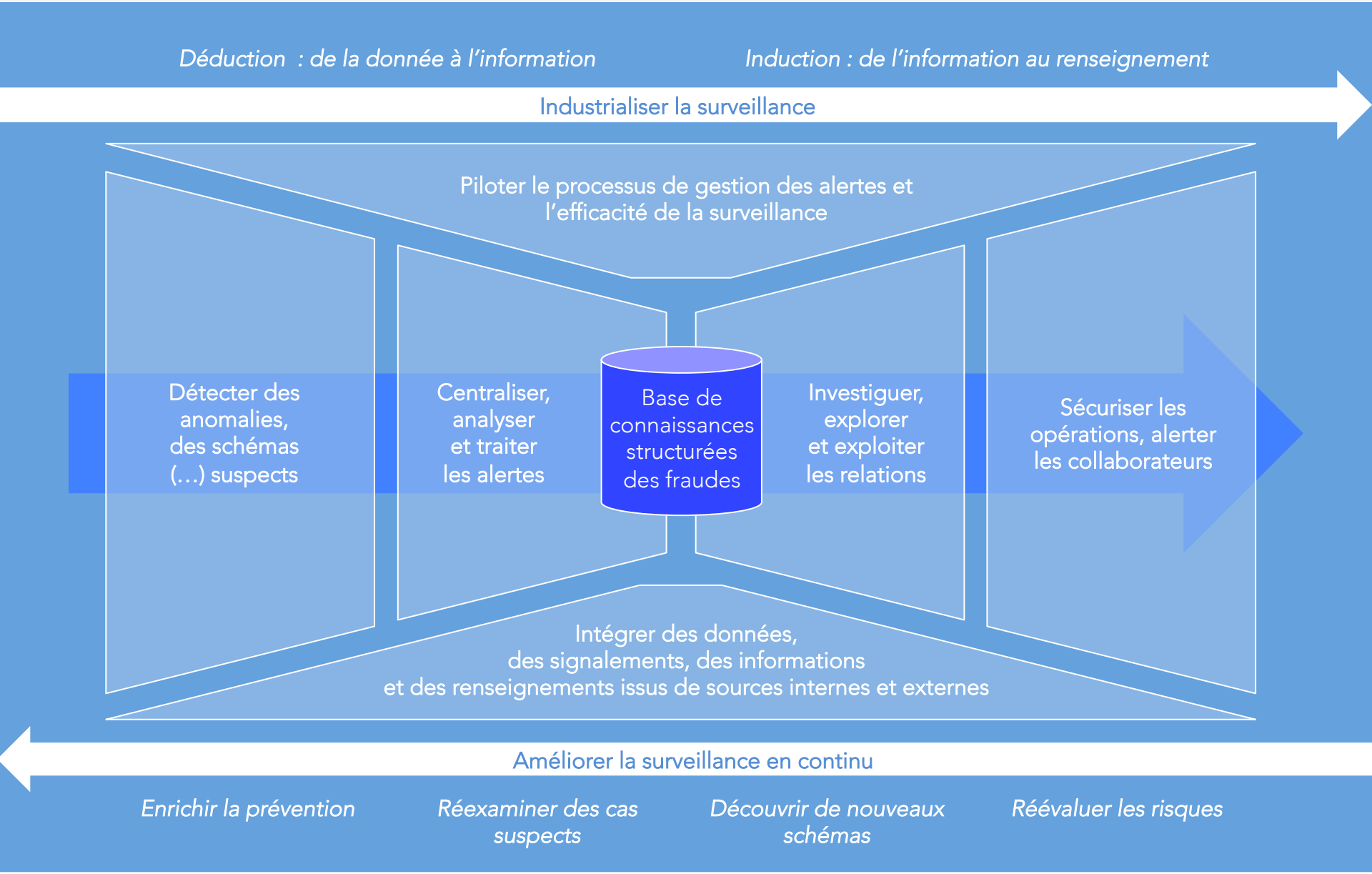
Industrialiser la surveillance



Deux clefs pour lutter efficacement contre les fraudes : 2) concevoir et gérer l'apprentissage



Lutter efficacement contre les fraudes nécessite de coordonner métiers, compétences et technologies.



Ne confondons pas une vision conceptuelle en apparence linéaire et une réalité plus complexe, plus exigeante, plus intégrée.

- La lutte contre les fraudes n'est pas un processus linéaire, un dispositif quasi-déconnecté qui s'inscrit en bout de chaine dans le business.

- Ce sont les singularités d'un métier (produit, canal de distribution, …), d'un système d'information, d'une organisation et d'une culture qui forgent une solution efficace.

- Le dispositif de lutte contre les fraudes doit être intégré aux processus métiers :
  - Octroi d'un crédit,
  - Indemnisation d'un sinistre automobile,
  - Accord préalable d'un remboursement (optique, dentaire, …),
  - Procédure d'entrée en relation bancaire,
  - Revue quotidienne des opérations suspectes dans un réseau bancaire.

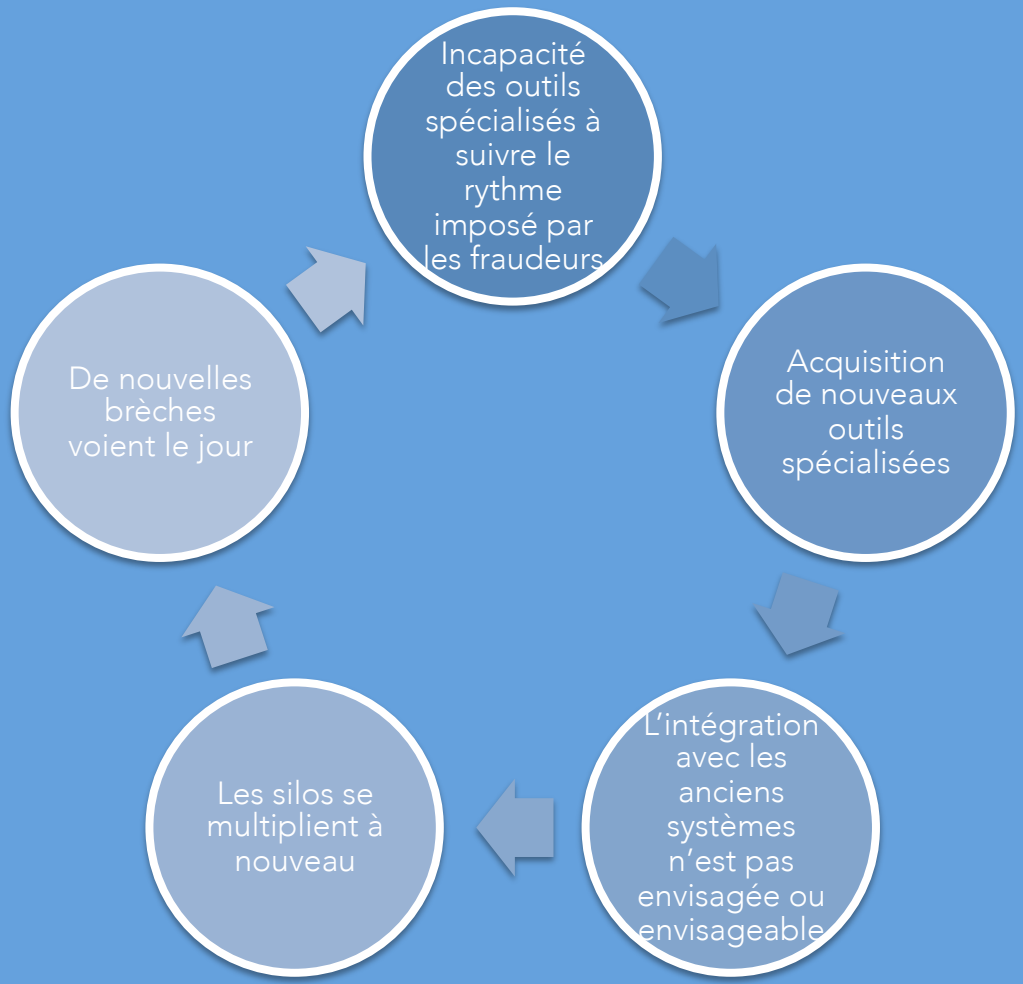
- Les éléments constitutifs de la lutte contre les fraudes doivent donc s'inscrire dans :
  - la culture d'entreprise,
  - les compétences des collaborateurs,
  - les tâches quotidiennes,
  - et le système d'information.

Capacités de lutte contre les fraudes des établissements : un constat révélant de sérieuses limitations

En 2013, un projet de lutte contre les fraudes ne part jamais de la page blanche …

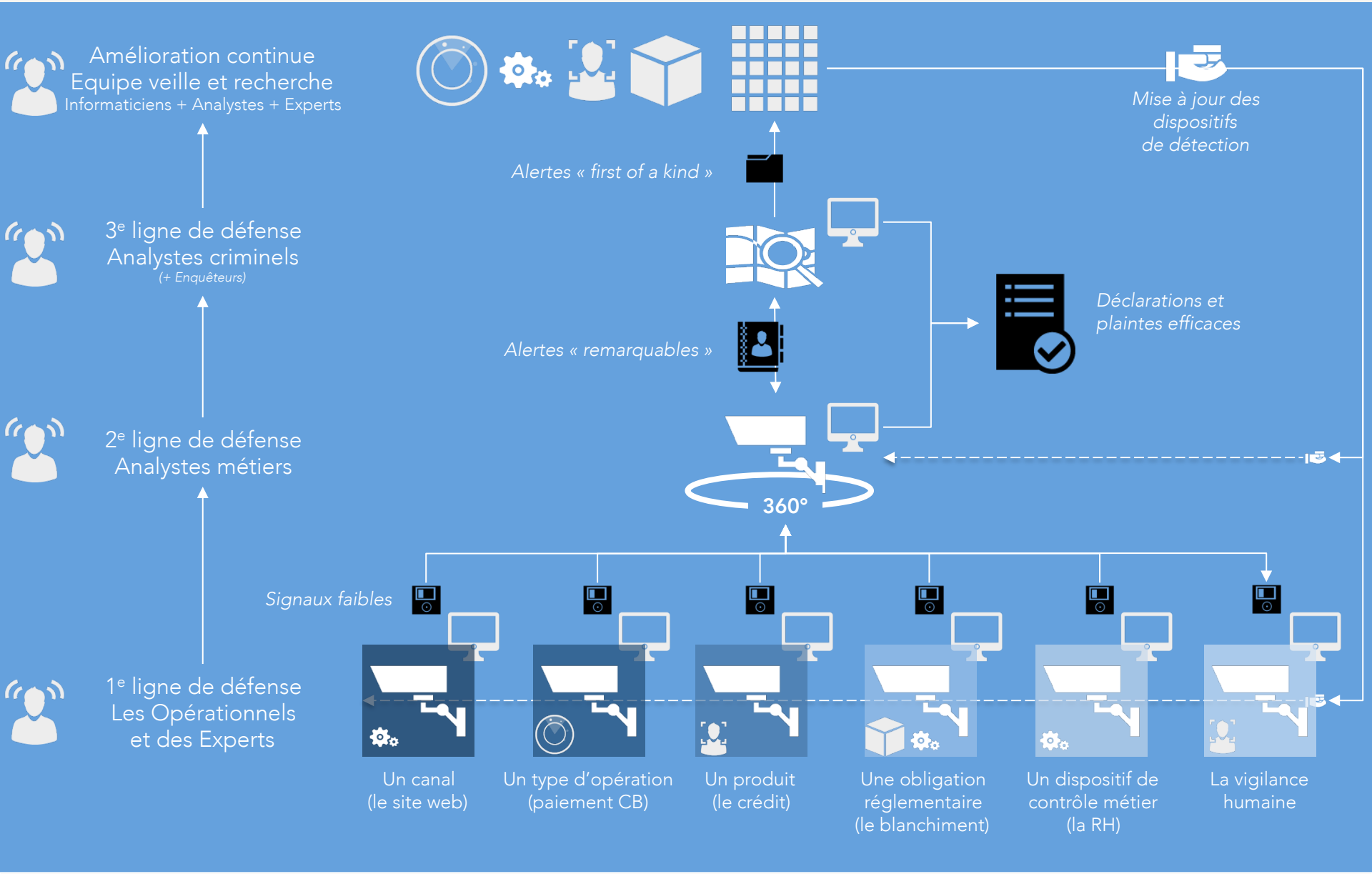
- Nombre d'organisations disposent déjà des capacités de lutte contre les fraudes : un savoir-faire, des compétences, des expériences, des outils.
- Mais, dans la grande majorité des cas, ils sont peu coordonnés et les outils en place ont atteint leurs limites :
  - **L'approche par silos** : les systèmes de lutte anti-fraude ont souvent été pensés pour combler une vulnérabilité, répondre à un besoin ciblé, une urgence.
    - Ils sont très efficaces (indispensables) mais il est difficile (impossible) de les faire évoluer et/ou d'étendre leur champ d'application.
  - **L'obligation continue d'innover est une ambition difficile à satisfaire** : Face aux nouvelles exigences imposées par la lutte contre les fraudes, la très grande majorité des éditeurs spécialisés (auteurs de progiciels d'ancienne génération) sont dépassés fonctionnellement, techniquement et financièrement.

… il convient donc de capitaliser et d'intégrer les différentes « briques » pour éviter la spirale infernale induite par la multiplication des techniques de fraudes …



Silos ou surveillance à 360° ? Les deux sont complémentaires.

Principaux flux d'information au sein d'une organisation de la lutte contre les fraudes



L'exigence d'intégration : des capacités informatiques de haut niveau

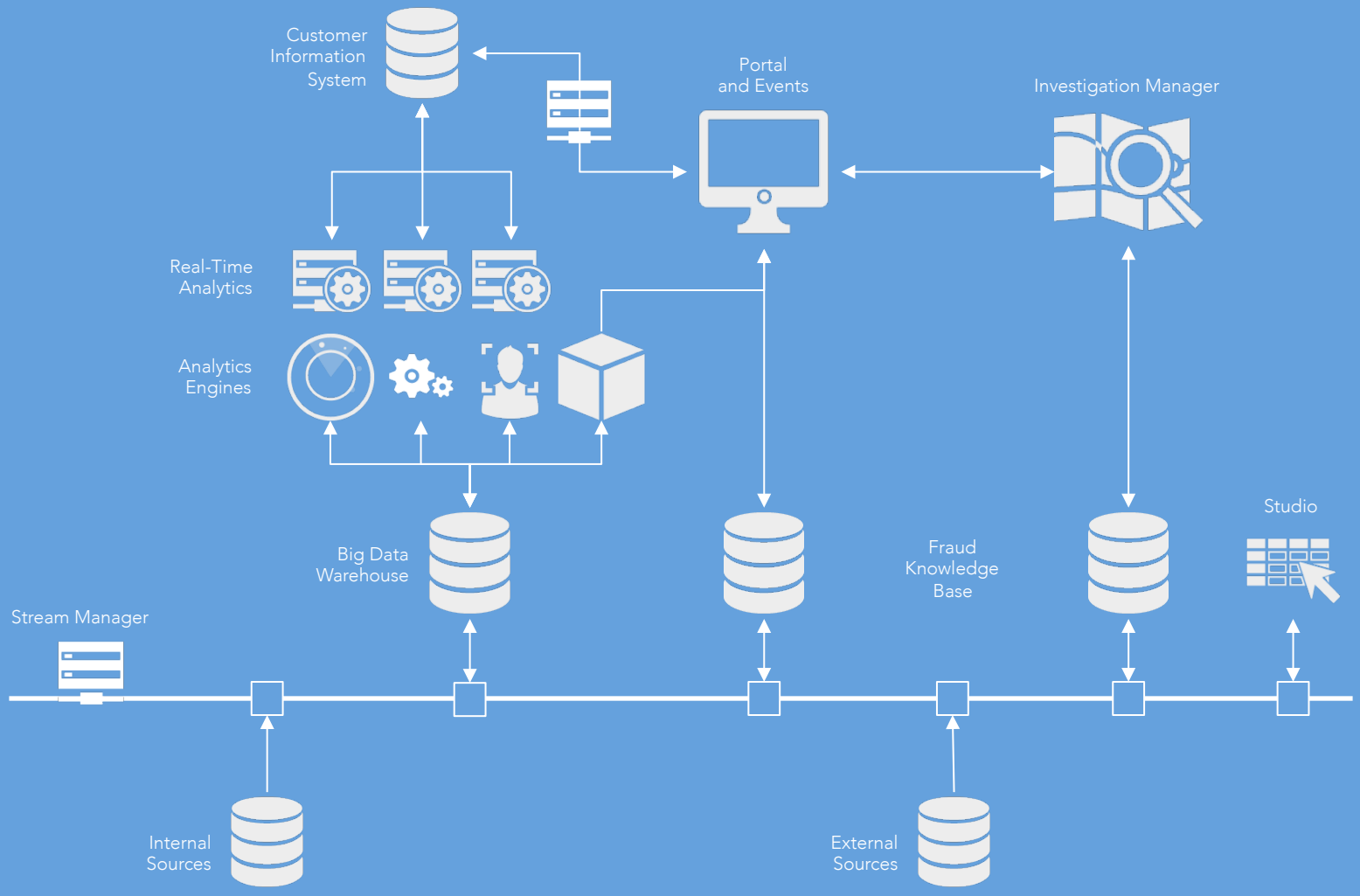
- Notre ambition : « Ne plus détecter les fraudes a posteriori mais a priori pour protéger l'établissement ou son client »

- En termes de capacités informatiques, les outils doivent donc :
  - S'adapter à l'organisation de l'établissement,
  - Répondre aux exigences des équipes de production informatique pour s'intégrer au sein des systèmes opérationnels,
  - Emettre des alertes a bon escient et permettre une collaboration intelligente entre les différents acteurs.

- Point de vigilance :
  - Lutter contre la fraude doit permettre de préserver la marge sans « tuer le business »

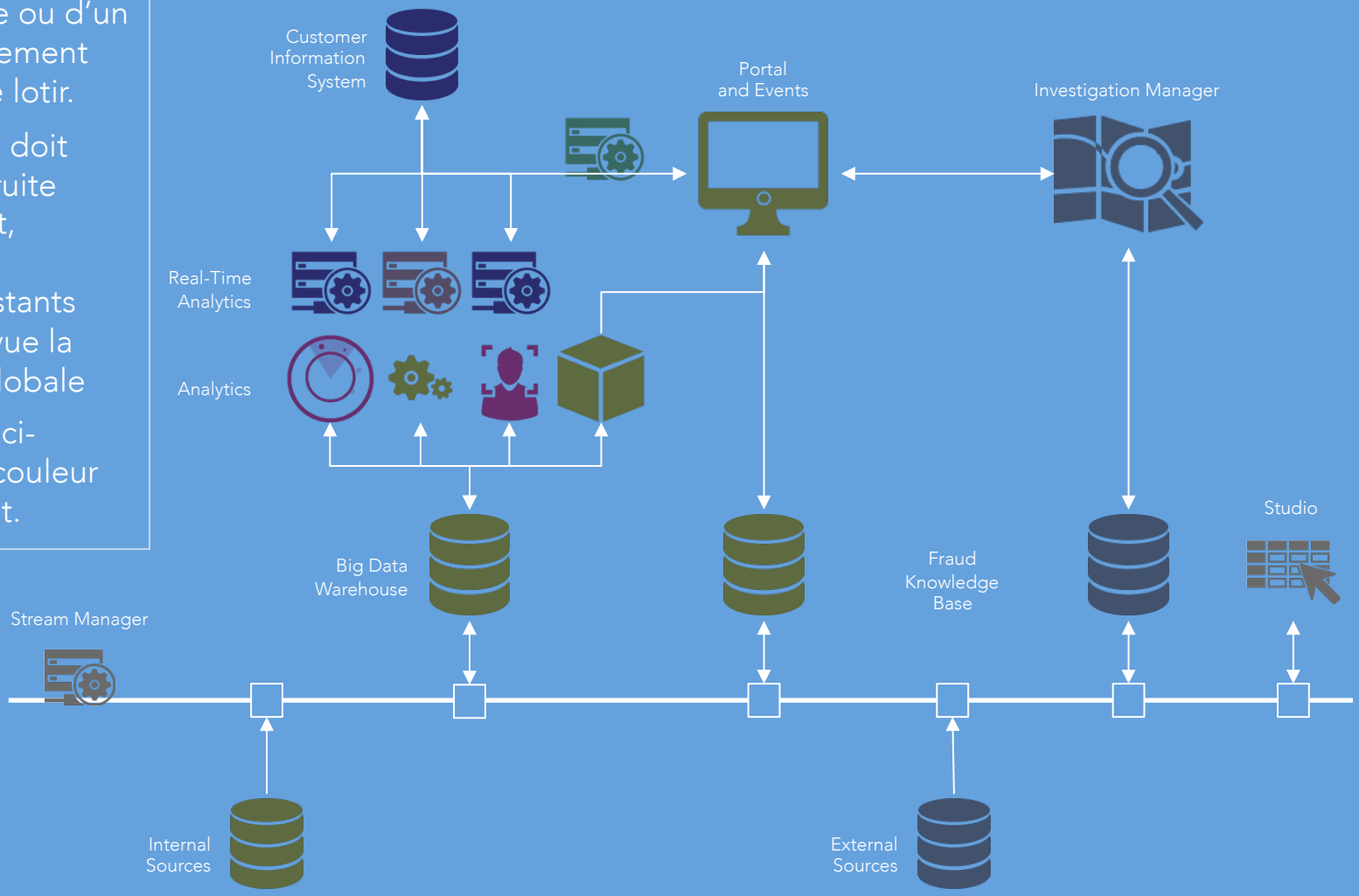
- Il est donc indispensable de maîtriser :
  - les performances techniques des outils (performances pures et disponibilité)
  - et les optimisations itératives des dispositifs de détection prédictive pour limiter les faux-positifs.

Une architecture rationnalisée de nouvelle génération : un premier parti pris …



… qui illustre parfaitement la nécessité de construire progressivement et néanmoins rapidement un dispositif global.

- Pour maîtriser les risques d'un programme ou d'un projet, il est fortement recommandé de lotir.
- La solution cible doit donc être construite progressivement, d'intégrer des composants existants sans perdre de vue la cible, la vision globale
- Dans le schéma ci-contre, chaque couleur représente un lot.



Les nouvelles compétences : un second parti pris

3e ligne de défense
Analystes criminels
(Enquêteurs)

- En 2004, la lutte contre le blanchiment annonce une nouvelle ère : de nouvelles obligations, de nouvelles charges.
  - Tracfin dans son dernier rapport incite les établissements à aller plus loin encore.
- « Aller plus loin » avec des analystes criminels capables de :
  - Mener des investigations poussées,
  - Percevoir des schémas complexes,
  - Mettre en évidence des failles et proposer des recommandations,
  - Paramétrer leurs propres outils d'analyse,
  - Communiquer clairement pour sensibiliser / alerter tous les acteurs,
  - Concevoir des dépôts de plainte efficaces.

Equipe veille et recherche
(Informaticiens + Analystes + Experts)

- Ajuster la surveillance :
  - quotidiennement, les opérationnels peuvent apprécier le risque d'un individu, le placer sous surveillance renforcée, ouvrir un plan d'action de lutte contre les fraudes …
  - … mais ils doivent aussi analyser les fraudes identifiées (ou signalées) pour ajuster les techniques de surveillance.
- Inviter les informaticiens car ils permettent :
  - de mener des études statistiques,
  - d'accélérer l'ajustement du dispositif,
  - de faciliter les tests empiriques indispensables et d'assurer l'intégrité du système d'information.

Les solutions analytiques : un troisième parti pris

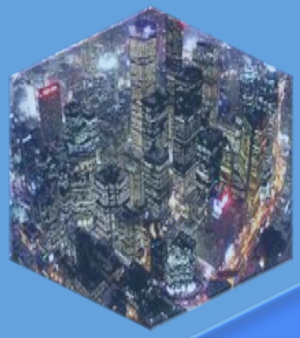
- **Text et Data Mining**
  - SPSS :
    - Analyse prédictive
    - La détection d'anomalies en temps réel (et en batch) sur des volumes très importants
    - Les techniques statistiques à la portée de tous

- **Entity Analytics**
  - IBM EAS
    - Résolution d'identités et de réseaux automatiques
    - Apprentissage continue automatique
    - Dictionnaire de noms
    - Fonctionne en temps réel et en batch

- **Rule Engine**
  - IBM ODM (ex-iLog)
    - Le langage naturel : La capacité à tester puis à déployer très rapidement des règles métier
    - Le déploiement de règles en temps réel (et en batch) sur des volumes très importants

- **Reporting et analyse multidimensionnelle**
  - IBM Cognos
    - Du reporting de masse à l'analyse multidimensionnelle pour vérifier ou découvrir des schémas indésirables
    - L'intégration avec les systèmes opérationnels pour gérer la visibilité

2013 – 2014 : les projets et les exigences de nos clients



Urbaniser

Oui aux silos s'ils sont synonymes d'expertise, d'efficacité ! Non aux silos s'ils piègent l'information !

Capturer les signaux faibles et les signalisations pour les exploiter et permettre de sécuriser

Disposer d'une vue à 360°

Moderniser Rationaliser

Remplacer des technologies anciennes et/ ou propriétaires par des technologies fiables ouvertes et évolutives

Former des équipes pluridisciplinaires et se doter d'analyse criminelle pour capter les schémas les plus complexes et rendre plus efficace le dépôt de plainte

Développer de nouvelles compétences

- Exigences de nos clients

  – Victoires rapides : Justifier un ROI à court terme demeure une exigence ;

  – Pérennité et évolutivité : Construire un système capable de supporter les exigences de demain.

Les challenges (induits) auxquels les éditeurs doivent faire face

Collecter et structurer un maximum de données, de signalisations, d'informations, de renseignements …

Intégrer des sources internes et externes systématiquement et à la demande

Gérer des volumes de données très importants et en rapide augmentation

… pour les analyser, les mettre à disposition des opérationnels, des analystes pour éclairer des décisions …

Analyser des données structurées et non structurées

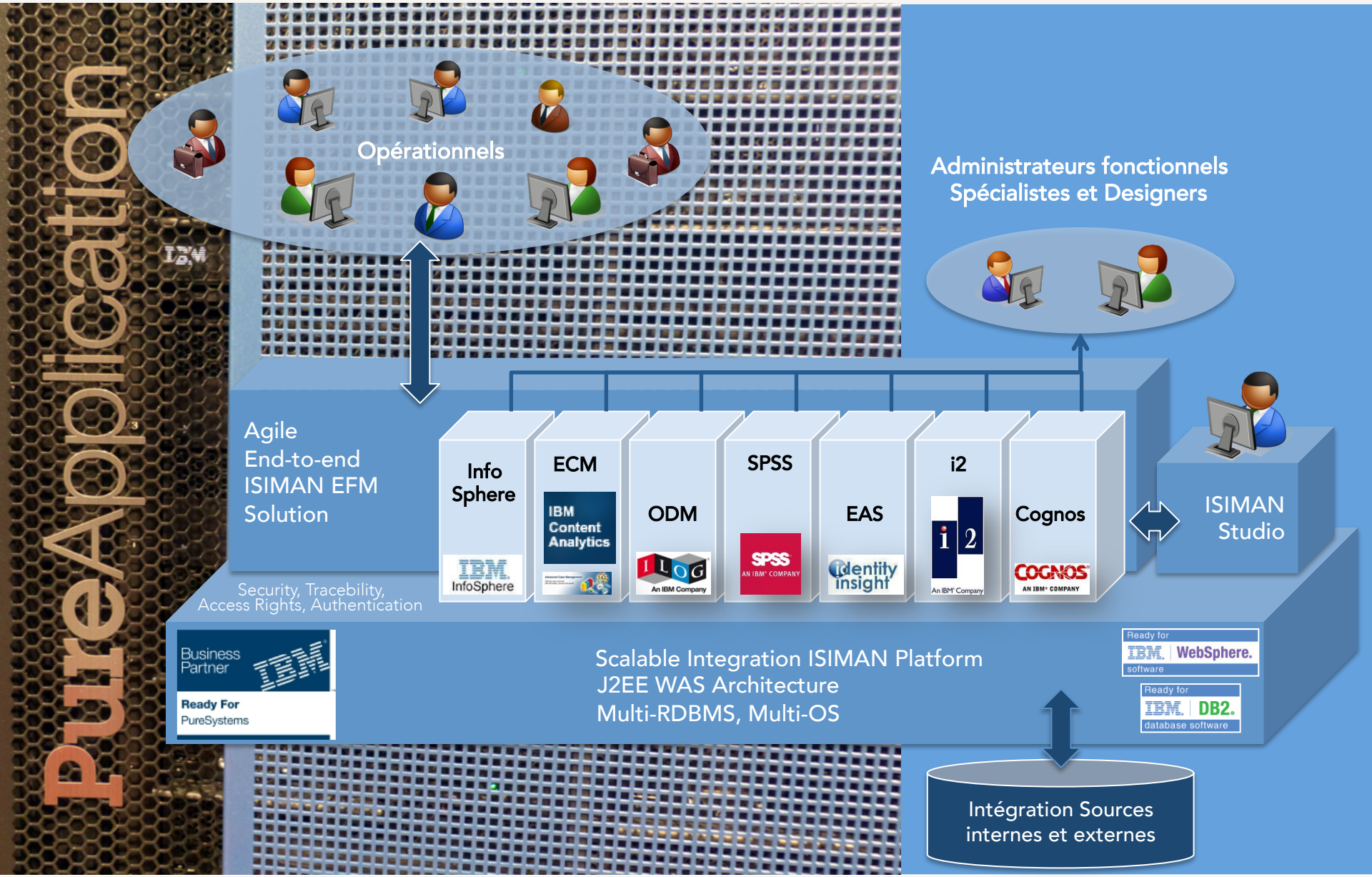
Réconcilier temps réel et décisionnel pour prévenir des fraudes

… et réduire le « time to detection » (temps qui sépare la conception d'une stratégie de surveillance de sa mise en production).

Concevoir un système apprenant, doté de capacités prédictives et le faire vivre

Réaliser une solution intuitive et agile à la main d'utilisateurs de plus en plus nombreux

ISIMAN EFM, un progiciel intégré de nouvelle génération « Ready for PureSystem, PureFlex, PureApplication »



Merci

ORUS advisors
A Keyword Group Company

DANIEL DELPUECH, DIRECTEUR GÉNÉRAL
KEYWORD GROUP
DANIEL.DELPUECH@KEYWORD.FR
04 67 07 72 00

FRANÇOIS JAUSSAUD, PARTNER
ORUS ADVISORS - KEYWORD GROUP
FJAUSSAUD@ORUSADVISORS.COM
06 30 99 34 03