EXPERIAN **INNOVATION FORUM** 2019

LA DATA AU SERVICE DE L'INNOVATION

24 octobre | Hôtel Le Casablanca, Maroc

experian™

Lutte contre la fraude

Évolutions et défis

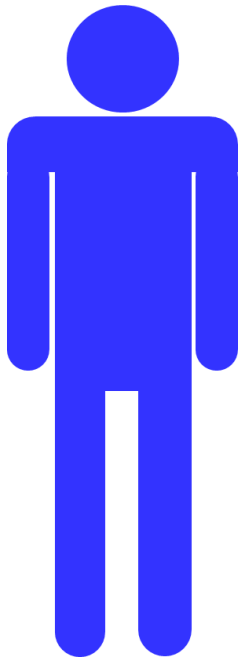
Frédéric DUBOUT

Senior Fraud Consultant EMEA, Experian

L’évolution de l’identité

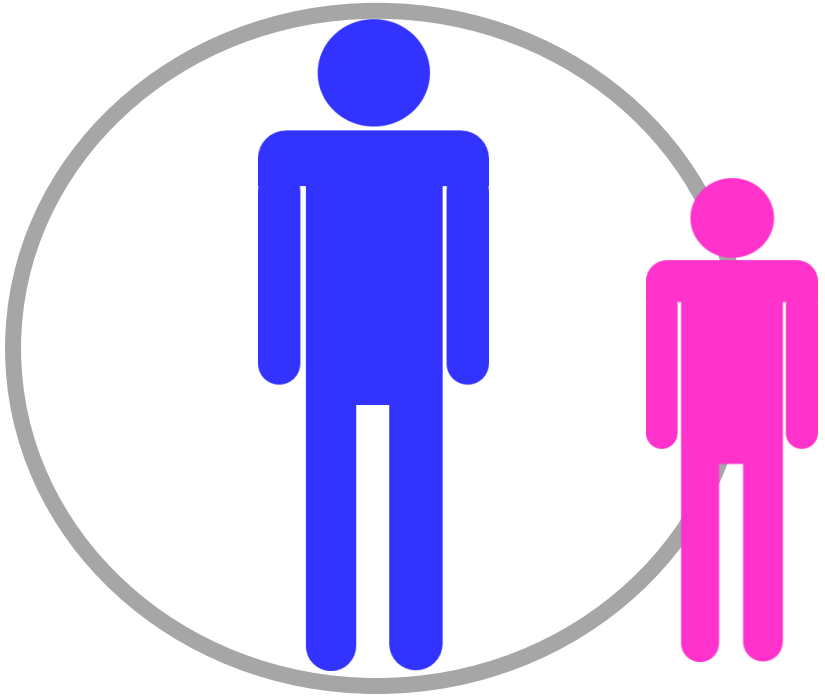
Dans un passé reculé

Identité =



L’évolution de l’identité

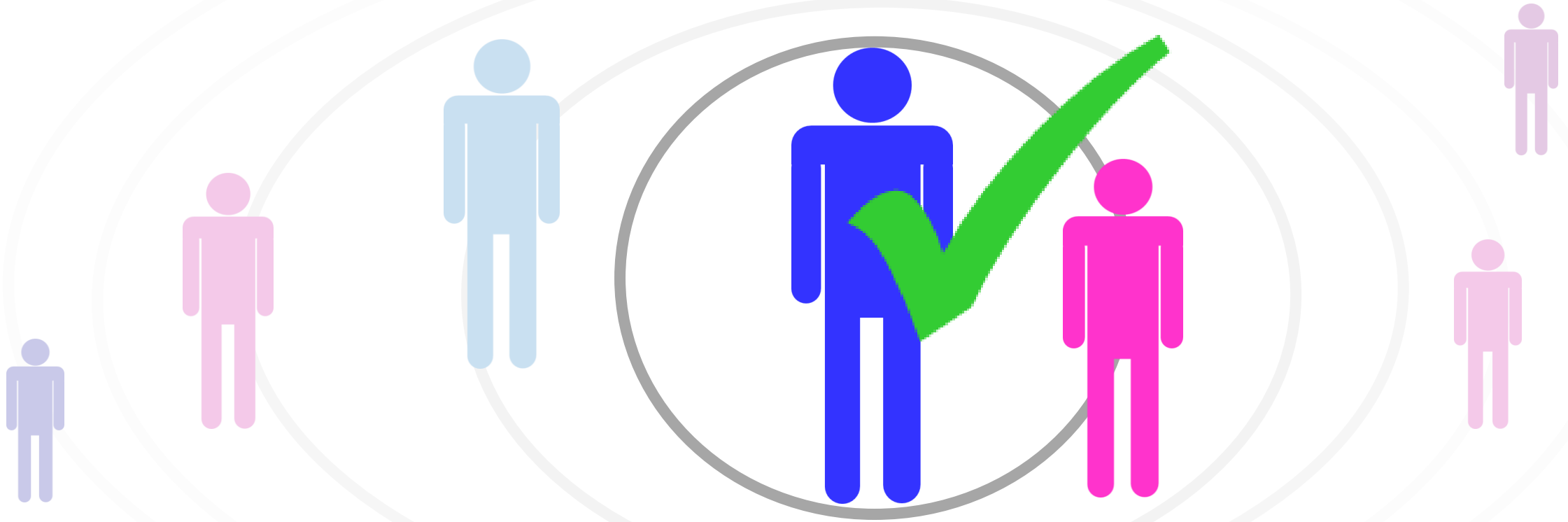
Dans un passé reculé



Vérification d’identité et business

L’évolution de l’identité

Dans un passé reculé

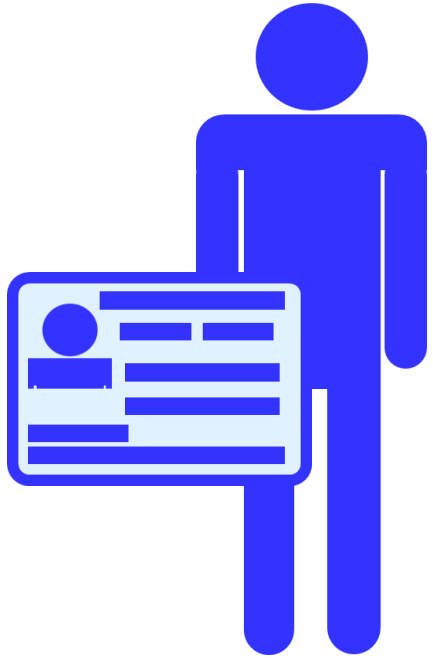


Vérification d’identité et business

L’évolution de l’identité

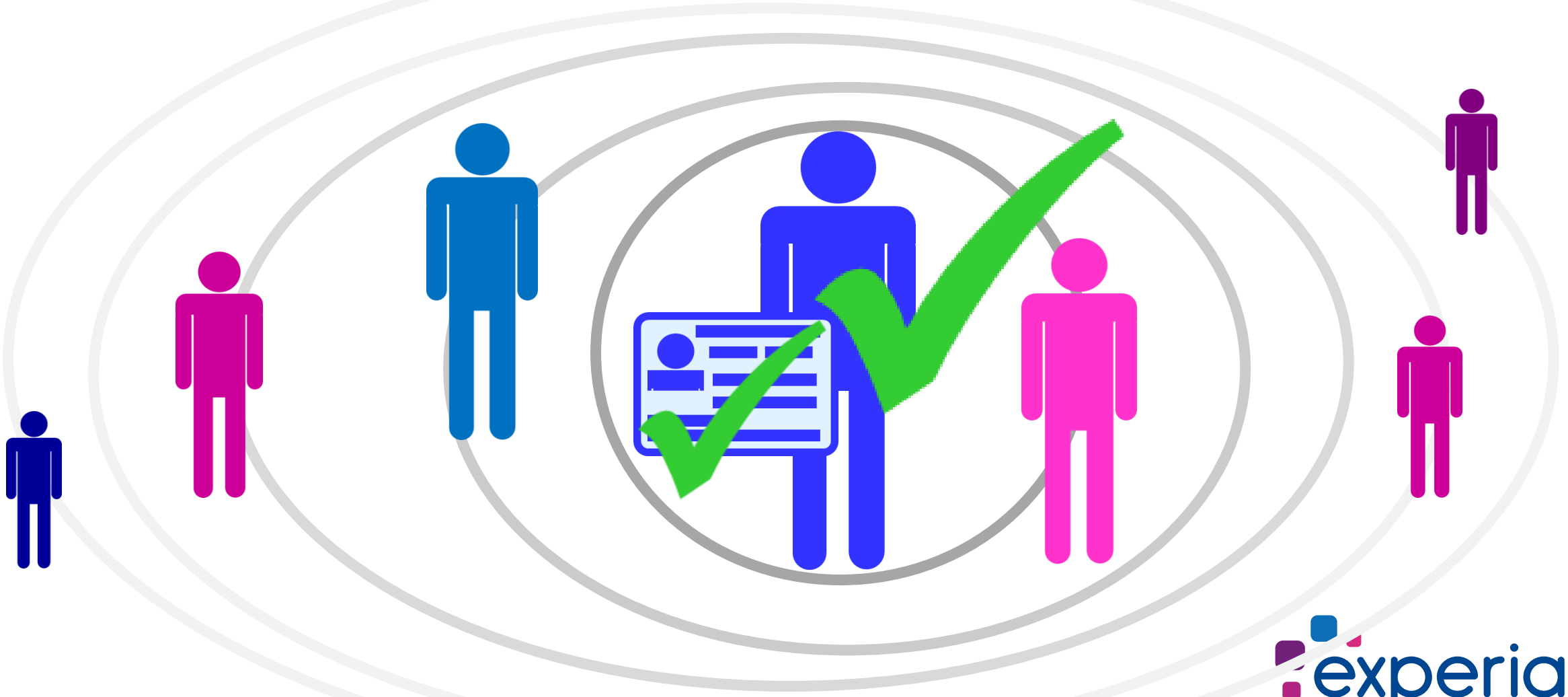
Du 18ème siècle à la fin du 20ème

Identité =



L’évolution de l’identité

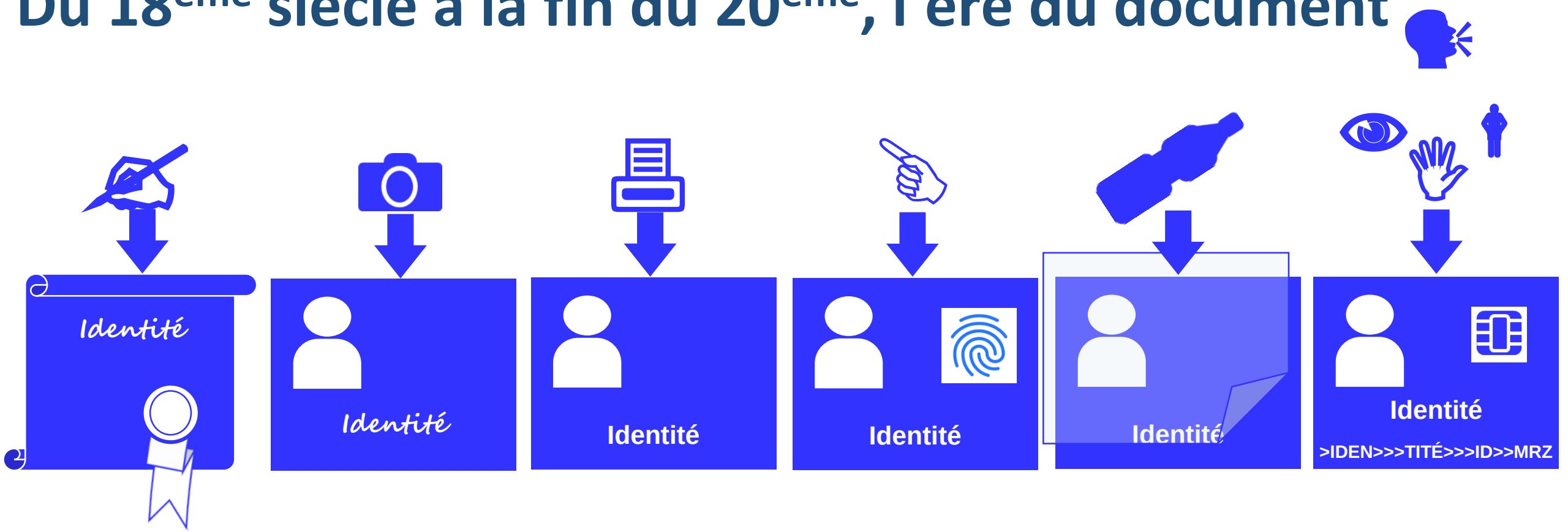
Du 18ème siècle à la fin du 20ème



Vérification d’identité et business

L’évolution de l’identité

Du 18ème siècle à la fin du 20ème, l’ère du document



Un jeu du chat et de la souris permanent contre les fraudeurs

L’évolution de l’identité

21ème siècle

Identité =

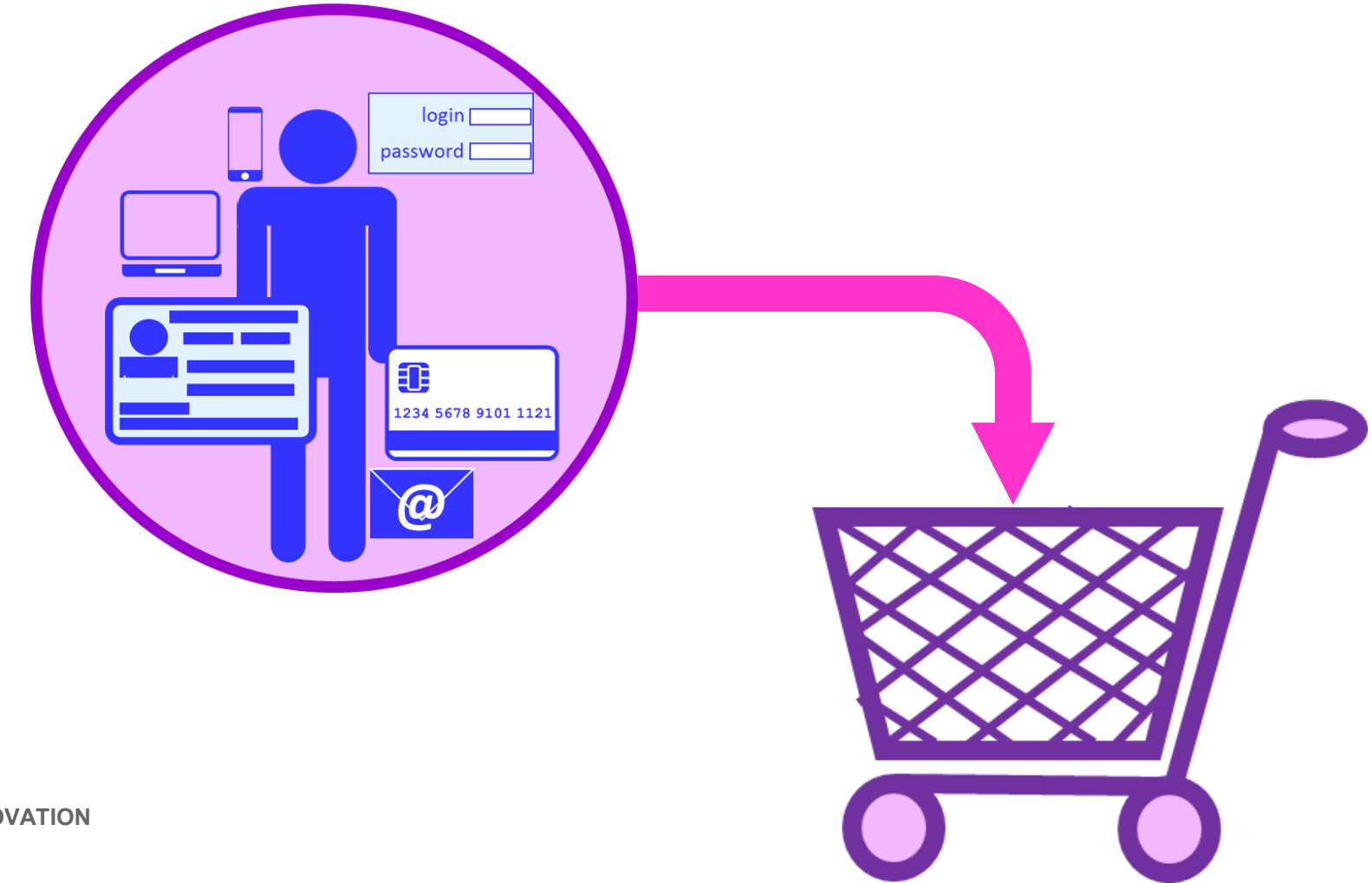
L’évolution de l’identité

21ème siècle

Vérification d’identité et business

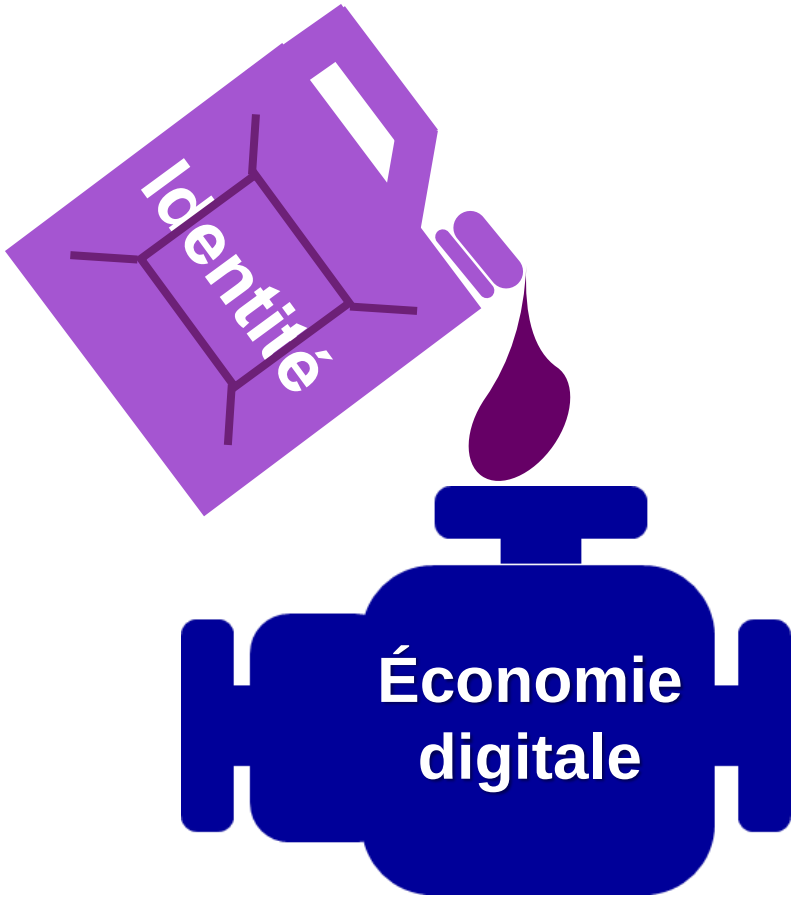
L’évolution de l’identité

L’identité est devenue une marchandise…



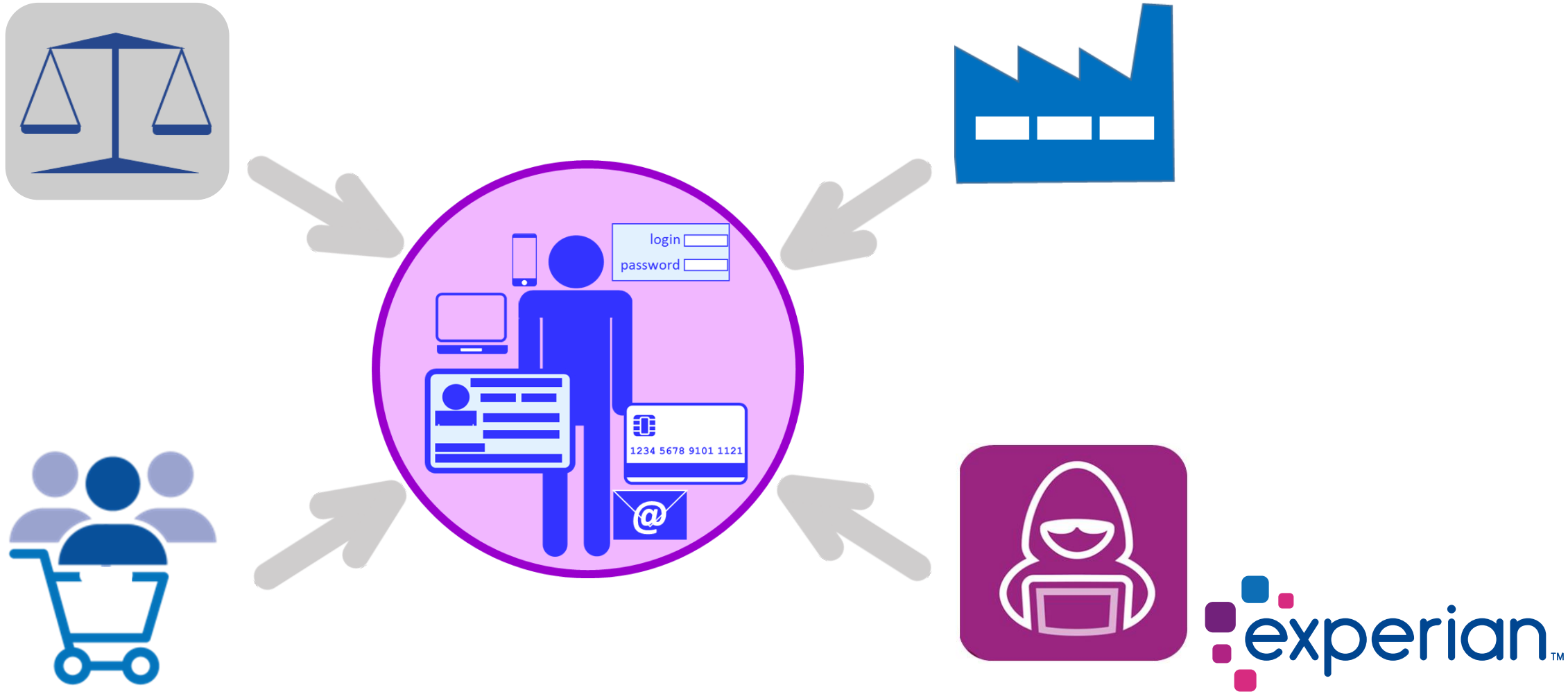
L’évolution de l’identité

…. Et cette marchandise est le carburant de l’économie d’aujourd’hui



L’évolution de l’identité

…. une marchandise très convoitée, et sous pression…



L’univers de l’identité est devenu une jungle

L’évolution de la fraude … les mêmes vieilles typologies…

Fraude à l’entrée en relation

- Ouverture de compte
- Demande de crédit
- Souscription
- Demande de carte

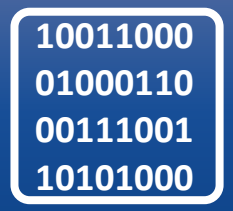
Usurpation de compte

- Banque
- Telco
- eCommerce
- Voyage et hospitalité
- Gambling
- Ticketing

Fraude transactionnelle

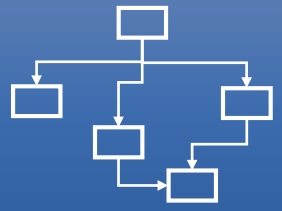
- Paiement carte
- Virement bancaire
- Modification de profil

L’évolution de la fraude …vieilles typologies, nouvelles méthodes



Évolution vers la cybercriminalité

Globalisée et sans frontière

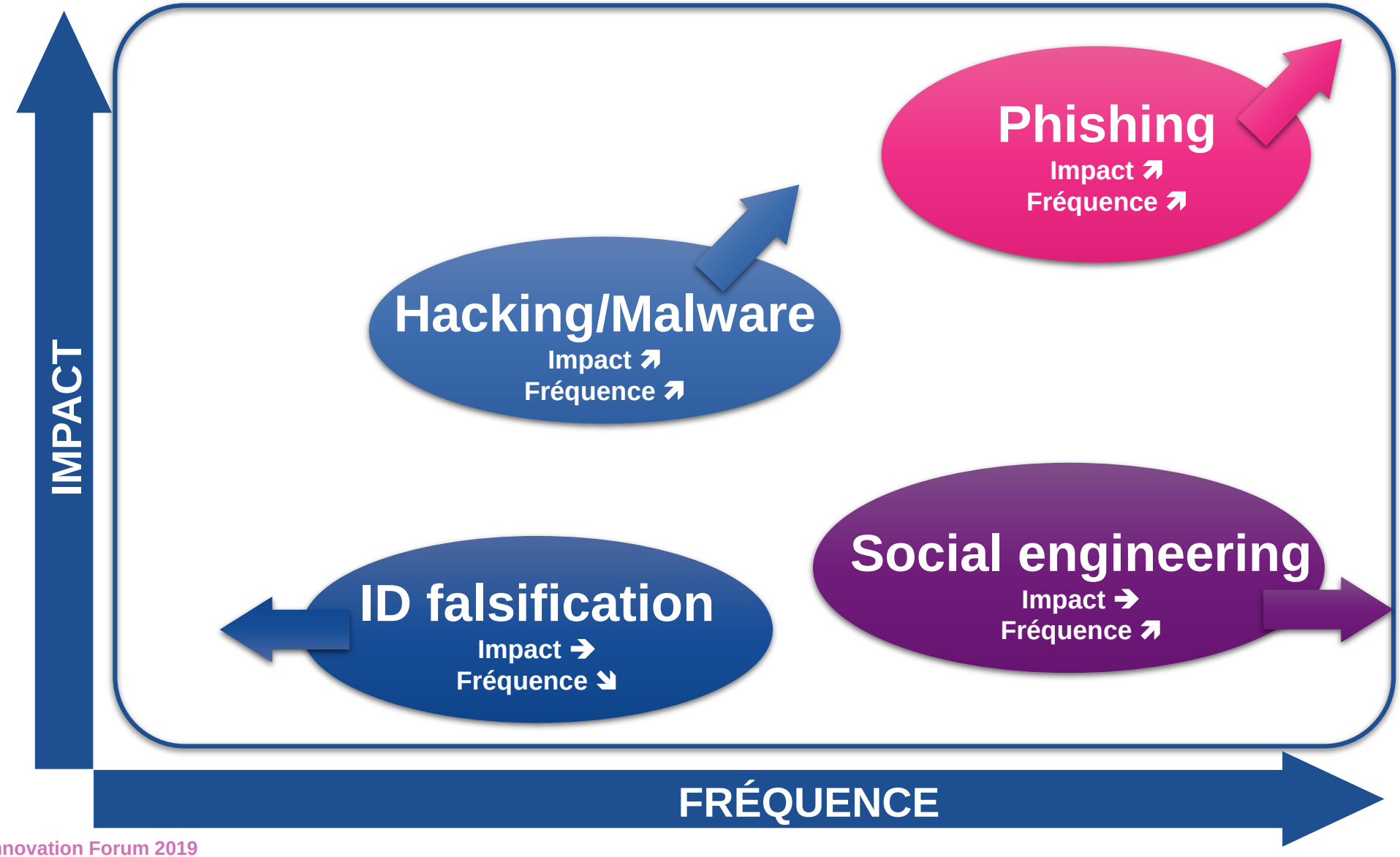


Structurée et sophistiquée

De l’artisanat à l’industrie

L’évolution de la fraude

Les techniques aussi évoluent



L’évolution de la fraude

Fraude et donnée: un cercle vicieux

La donnée est le nouvel or noir, carburant de l’économie d’aujourd’hui
...et est donc attractive pour les fraudeurs

Les vols de données alimentent les stocks disponibles à la vente

Les stocks abondants et bon marché alimentent la fraude

La fraude sape la confiance entre entreprises et consommateurs

Pas convaincus?... quelques chiffres

Depuis 2005

9 033 fuites massives de données*

11 582 milliards d'enregistrements

Rythme actuel

291 enregistrements/sec **

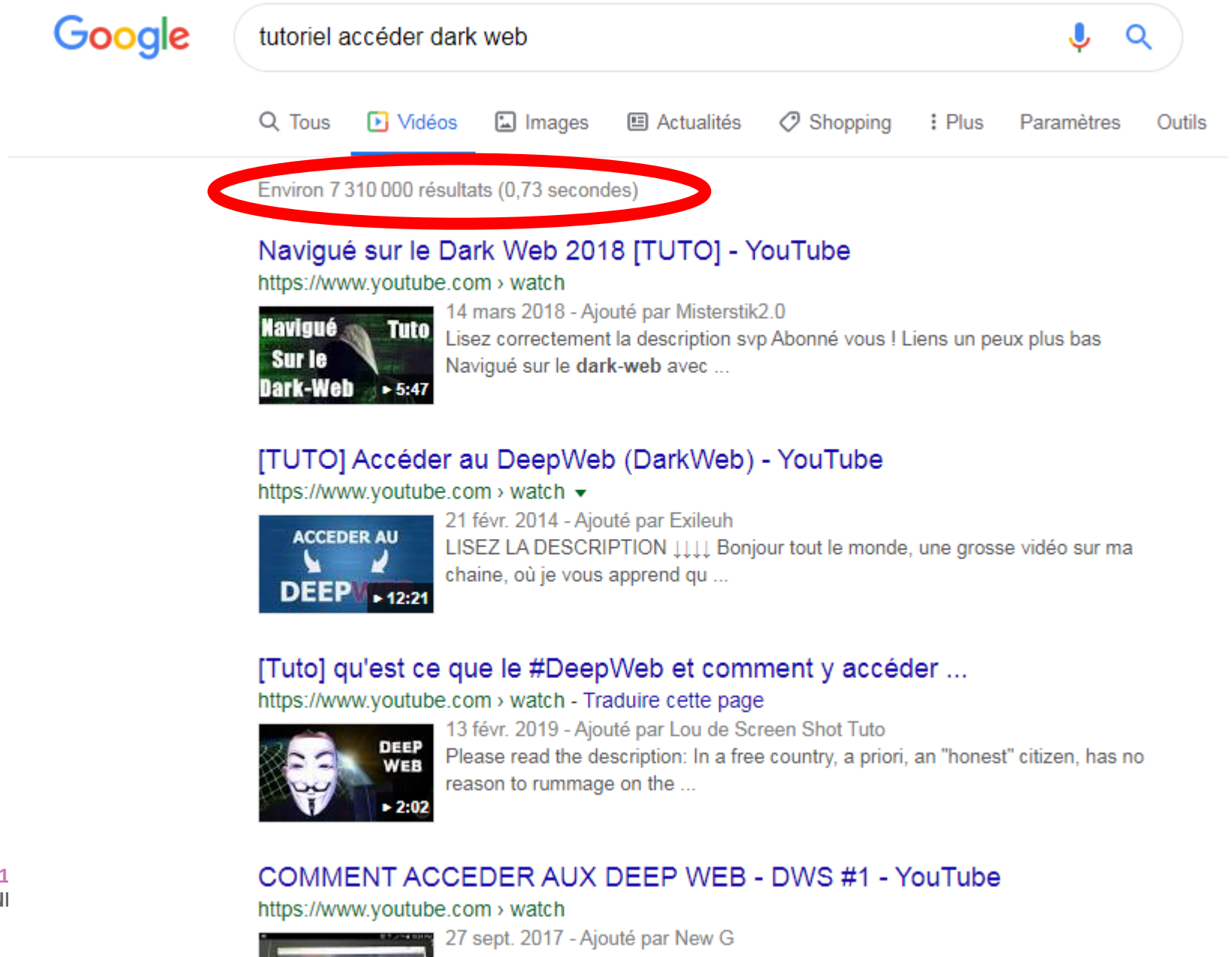
…en comptant seulement les fuites majeures…

…maintenant, imaginez l'addition des cas de phishing…

* source: www.privacyrights.org

** source: Malwarebytes

Compliqué d'aller sur le dark web?... Pas sûr....

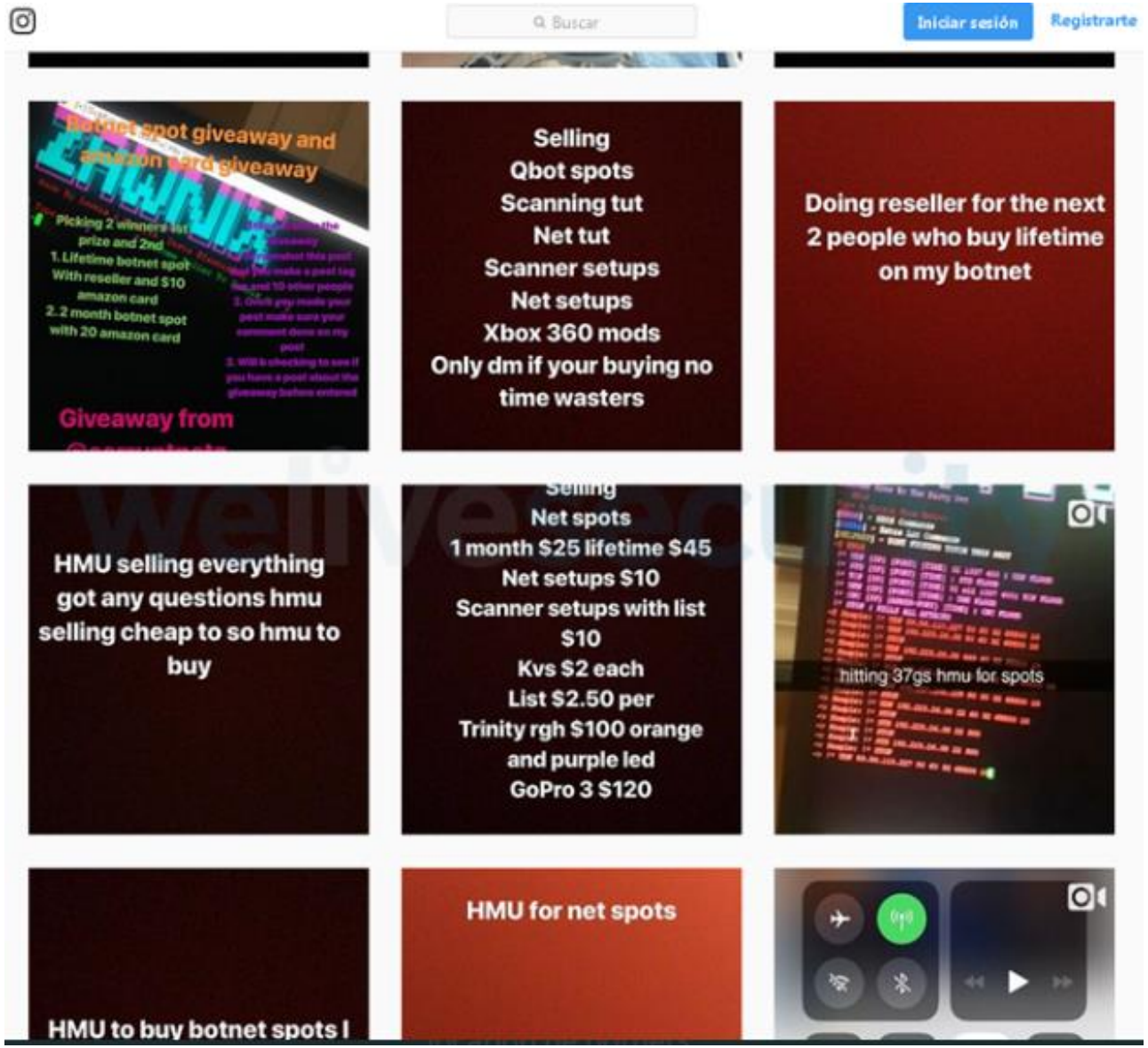


Compliqué et cher d'utiliser un malware?... Pas sûr….

-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	**12**
Price	120 USD	490 USD	900 USD	1900 USD

Vraiment obligé d'aller sur le Dark Web?....pas sûr....



...un compte Instagram devrait suffire...

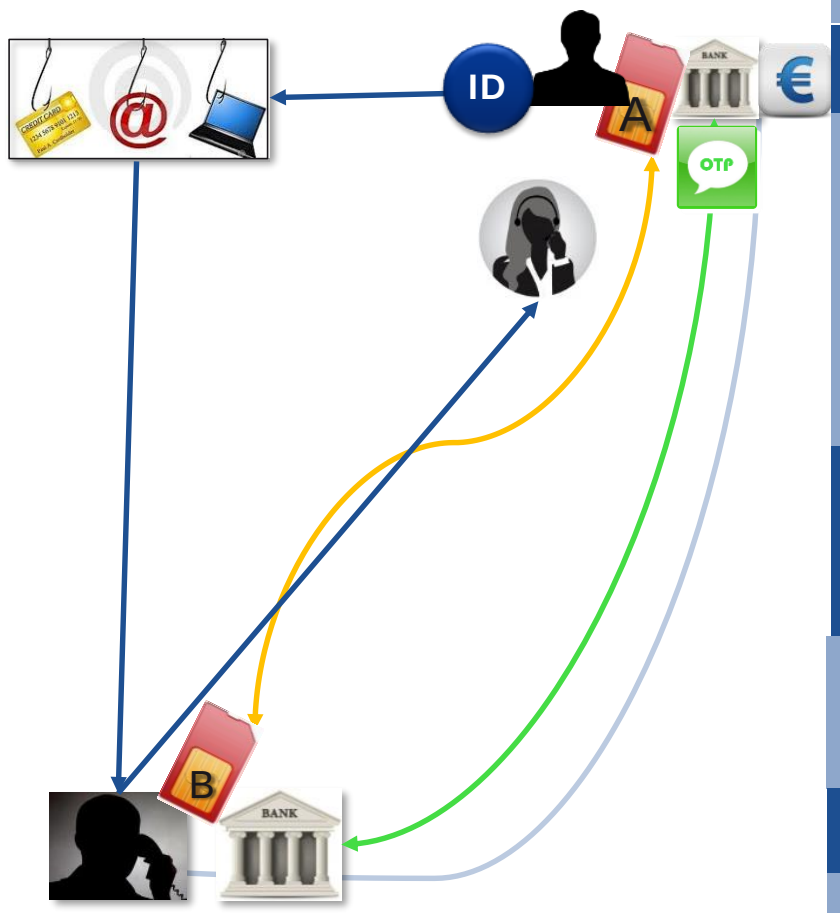
L’investissement est trop important?....pas sûr….

FULLZ	50-120 €
Credentials banque	60-80 €
PAN + CVV carte	20-50 €
Scan de passeport	10-12 €

…prix dégressifs, et parfois…

…satisfait ou remboursé…

Contournement d'authentification. Méthode 1: SIM SWAP



Le fraudeur se procure des cartes SIM postpaid au marché noir

Utilise le phishing pour voler identifiants bancaires et téléphone

Usurpe l'identité pour obtenir un SIM SWAP sur la ligne de la victime

Une fois le SIM SWAP obtenu, la SIM de la victime (A) est déconnectée du réseau et n'en est plus reconnue, alors que celle du fraudeur (B) est authentifiée par le réseau et autorisée à émettre et recevoir appels et sms sur le numéro de la victime.

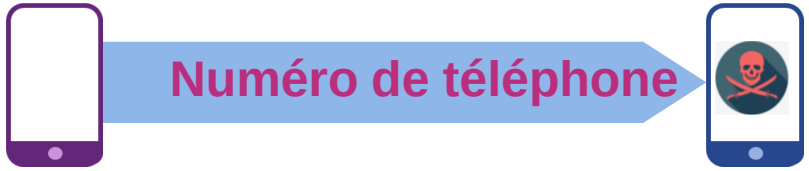
Le fraudeur se connecte à l'espace banque en ligne de la victime et initie un virement vers un nouveau bénéficiaire (compte de mule)

La banque envoie un challenge (OTP sms) à son client…reçu par le fraudeur

…qui s'authentifie aisément

.. La banque procède au virement vers le compte de mule

Détournement d’authentification. Méthode 2: fraude portabilité



Le fraudeur a préalablement volé les identifiants bancaires et le numéro de téléphone de sa victime (par phishing, social engineering).

Le fraudeur va souscrire une nouvelle ligne mobile, prétendant être la victime, et demande à conserver son numéro, il fournit le numéro de sa victime

Cela déclenche l’envoi d’un code de portabilité vers la victime (par sms)

Le fraudeur obtient ce code par social engineering (ex: appelle la victime en se faisant passer pour son NO et demande à vérifier le code pour des raisons de sécurité

Quelques heures ou jours plus tard, la victime est déconnectée du réseau. Au même moment le fraudeur peut envoyer et recevoir via le numéro porté.

Le fraudeur initie une transaction depuis le compte de la victime. La banque envoie un challenge à son client (OTP SMS).

…reçu par le fraudeur…qui satisfait l’authentification et finalise la transaction. La banque transfère l’argent vers le compte défini par le fraudeur (compte de mule)

Détournement d'authentification. Méthode 3: malware

Le fraudeur utilise un drive-by malware qui épie les connections à la banque en ligne de la victime. Il le place dans des bannières de sites web, via des liens dans des emails, etc…. La victime le télécharge et l'installe à son insu.

Le PC de la victime est sous contrôle d'un serveur C&C. Les identifiants sont volés. Le malware insère une iframe dans une page du site bancaire. L'iFrame invite la victime à donner son numéro de téléphone (+ modèle), sous prétexte de sécurité.

La victime reçoit un faux sms de sécurisation avec un lien vers un pseudo certificat (qui est en fait un autre malware). Ce malware a pour but de rediriger tous les sms envoyés par la banque vers un autre numéro (à l'insu de la victime).

Le fraudeur initie alors une transaction depuis le compte de la victime, vers un compte de mule.

La banque envoie un challenge à la victime, pour authentifier la transaction (un sms OTP). Le sms est re-routé vers la ligne possésée par le fraudeur.

…le fraudeur passe aisément le challenge et mène la transaction à bien

..la banque transfère l'argent vers le compte de mule défini par le fraudeur

Questions

Avez-vous encore confiance en l'authentifcation par OTP sms?

Quelle confiance dans les Sécuripass Certicode , Mobile Connect et autres authentifications OOB?

Quel est le niveau de friction généré par ces protocoles?

Et surtout…

Quelle confiance avez-vous en vos clients face au social engineering?

Notre réponse: le modèle Experian de prévention de la fraude

Exploitation des sources de données disponibles

- Information fournie par le client (déclaratif)
- Données présentes sur les documents d'identité
- Analyse du device et du contexte de connexion (pour le canal digital)

Prévention sur différents processus et points du cycle de vie:

- **Entrée en relation**
  - Ouverture de compte
  - Demande de prêt
  - Demande de carte
- **Gestion des comptes existants**
  - Accès aux comptes (au niveau page login)
  - Transactions initiées à partir des comptes
    - Virements
    - Modifications de profil

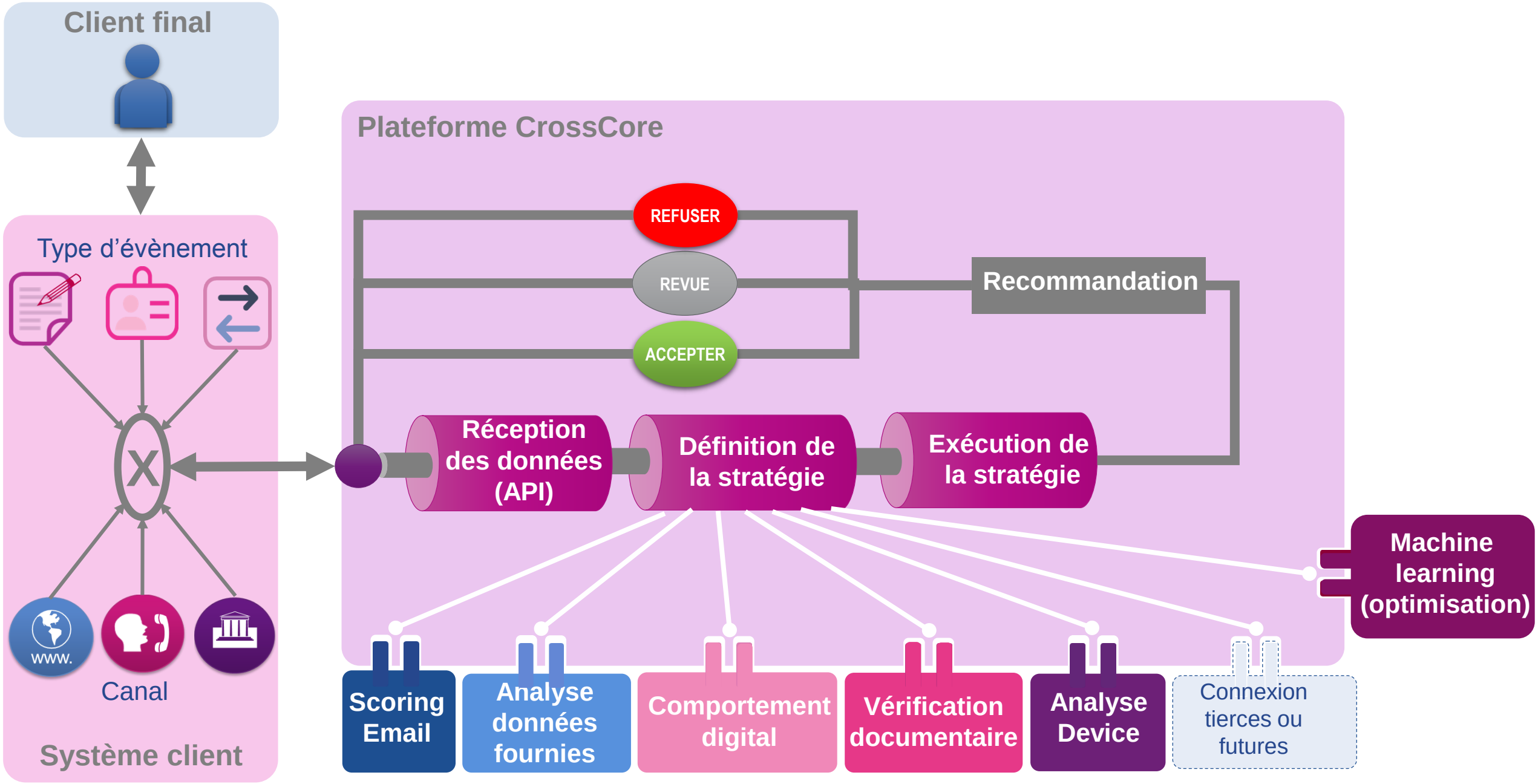
Fourniture d'outils adaptés:

- Plateforme (point d'entrée unique)
- Gestion de stratégies (géométrie variable)
- Approche modulaire (device, email, documents, données)
- Console (case manager) d'investigation et traitement

Protection multi-canaux

- Présentiel
- Téléphone
- Digital

Notre réponse: Crosscore, une plateforme ouverte



Et demain?... le RPA (Robotic Process Automation)

Augmenter la productivité

Améliorer la qualité

Optimiser l'allocation des ressources