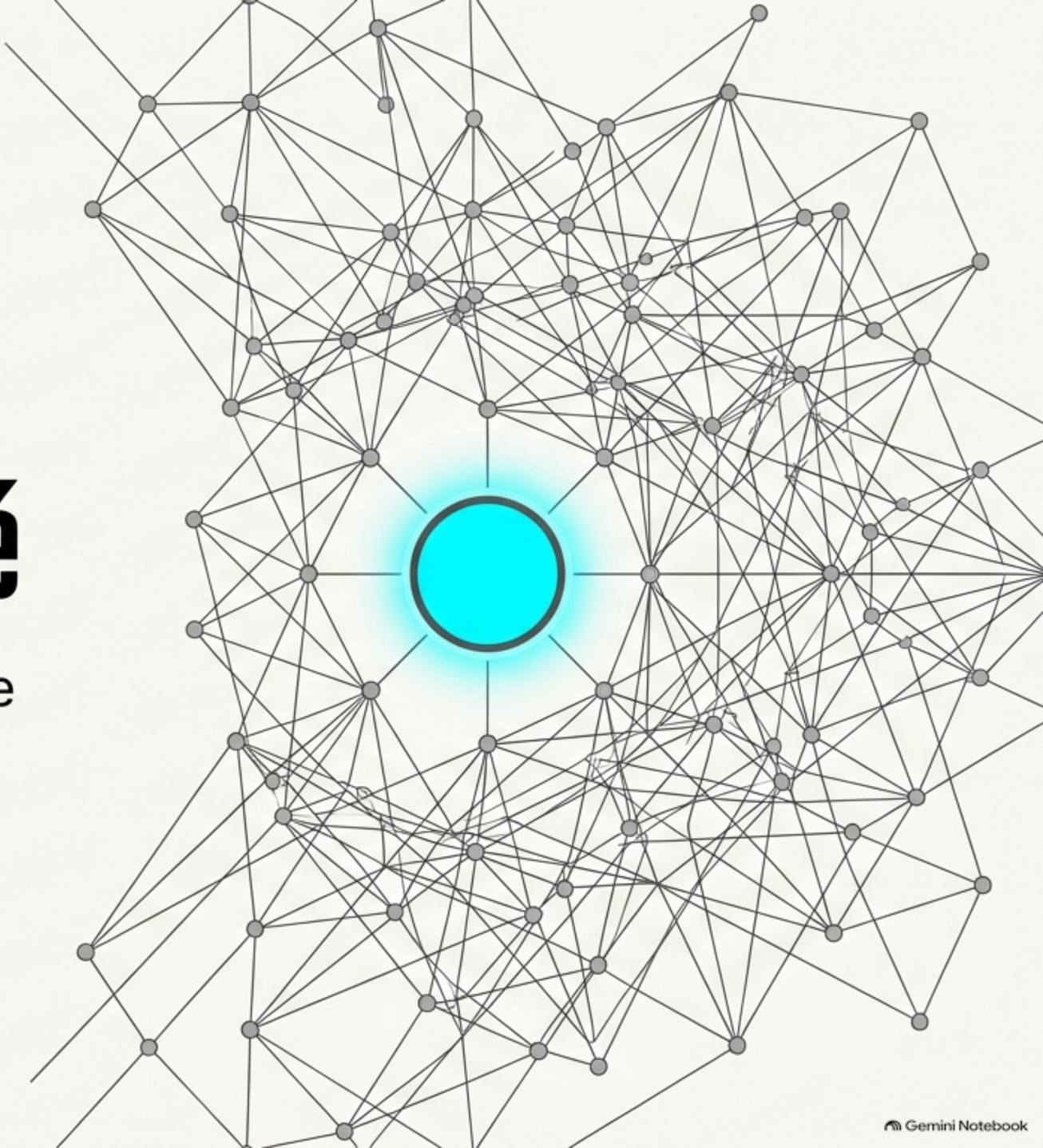
Pacta Cyber Lab : L'Humain au Cœur de la Cybersécurité

Sensibilisation, Investigation Numérique et Formation à l'Informatique.

Alain STEVENS - Pacta.com - Pacta Labs



Le Paradoxe de la Sécurité Numérique

L’Illusion Technologique

Notre système est techniquement impénétrable.

Les pares-feux, antivirus et chiffrements sont robustes. Les criminels ne s’attaquent plus frontalement aux machines.

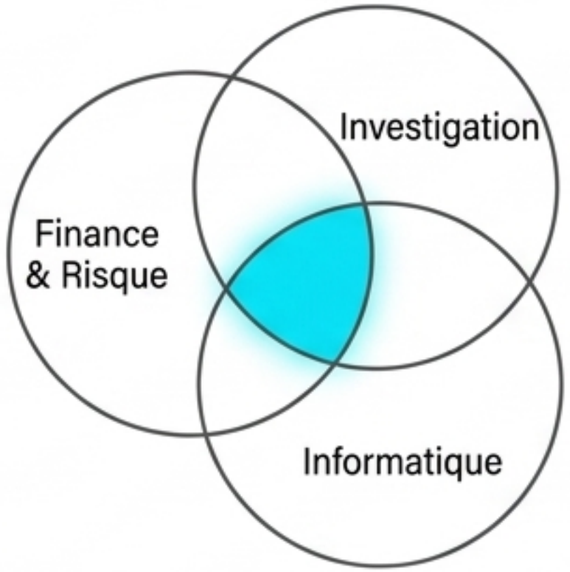
La Faille Humaine

La **Faille Humaine**

Les cybercriminels manipulent les utilisateurs pour qu’ils ouvrent la porte eux-mêmes.

Les leviers de l'ingénierie sociale :
- L'Urgence
- La Peur
- L'Autorité
- L'Appât du gain

Les Origines : De l’Enquête Financière au Cyberdétective



Avant 1999 (Banque & Finance)

Première école du risque. Apprentissage de l'analyse des anomalies, des données structurées et de la détection de la fraude avant que l'incident ne survienne.

1999 (Le Tournant Numérique)

Création de l'agence à Cannes.
Pionnier de l’investigation sur Internet.
Reconnu par la presse sous le terme de Cyberdétective.

Aujourd’hui (Pacta Cyber Lab)

Application des méthodes rigoureuses d'enquête traditionnelle à la complexité numérique moderne et à la prolifération de l'IA.

Une approche forgée bien avant l'explosion de l’OSINT, basée sur un principe constant : vérifier la donnée avant de prendre une décision.

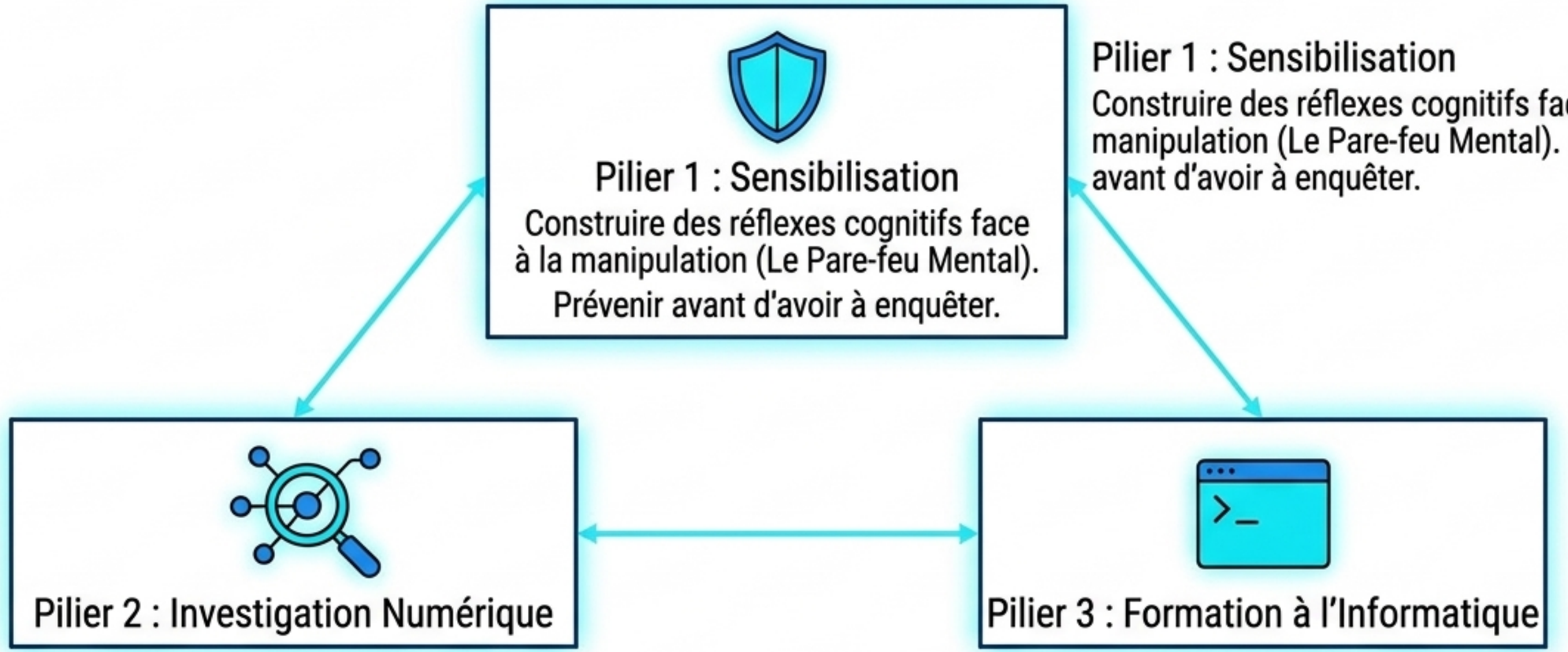
Deux Approches Complémentaires de la Cybersécurité

	Ingénierie Classique	Pacta Cyber Lab
Domaine d'expertise	Le Réseau et l'Infrastructure.	L'Humain et l'Information.
Menace ciblée	Vulnérabilités logicielles, failles réseau.	Ingénierie sociale, manipulation, fraude, désinformation.
Action préventive	Configuration, Pentest, Chiffrement.	Sensibilisation, construction du Pare-feu mental, réduction de la complexité.
Action curative	Restauration système, Patch de sécurité.	Investigation numérique (OSINT), rapprochement d'indices, identification des traces.

L'ingénierie seule ne suffit pas. Protéger la machine est inutile si l'humain cède ses accès.

La Méthodologie Pacta Cyber Lab

Un triptyque pour une maîtrise totale du risque numérique.



Pilier 1 : Sensibilisation

Construire des réflexes cognitifs face à la manipulation (Le Pare-feu Mental). Prévenir avant d'avoir à enquêter.

Exploiter l'OSINT pour collecter, vérifier et relier les traces. Découvrir qui se cache vraiment derrière l'écran.

Comprendre la machine, coder ses propres outils et réduire sa dépendance aux solutions externes.

Pilier 1 : Sensibilisation et Pare-feu Mental

Le concept

Développer des réflexes pour ralentiir la décision. Ne plus considérer automatiquement l'écran comme une vérité absolue.

La menace amplifiée

L'IA industrialise la tromperie, rendant les textes parfaits, les voix imitées et les images de synthèse indiscernables de la réalité.

L'Objectif

Transformer l'utilisateur, souvent perçu comme le maillon faible, en une véritable première ligne de défense active.

Pilier 2 : Investigation Numérique (OSINT)

L’art de faire parler les traces numériques.

La Méthode de l’Enquêteur

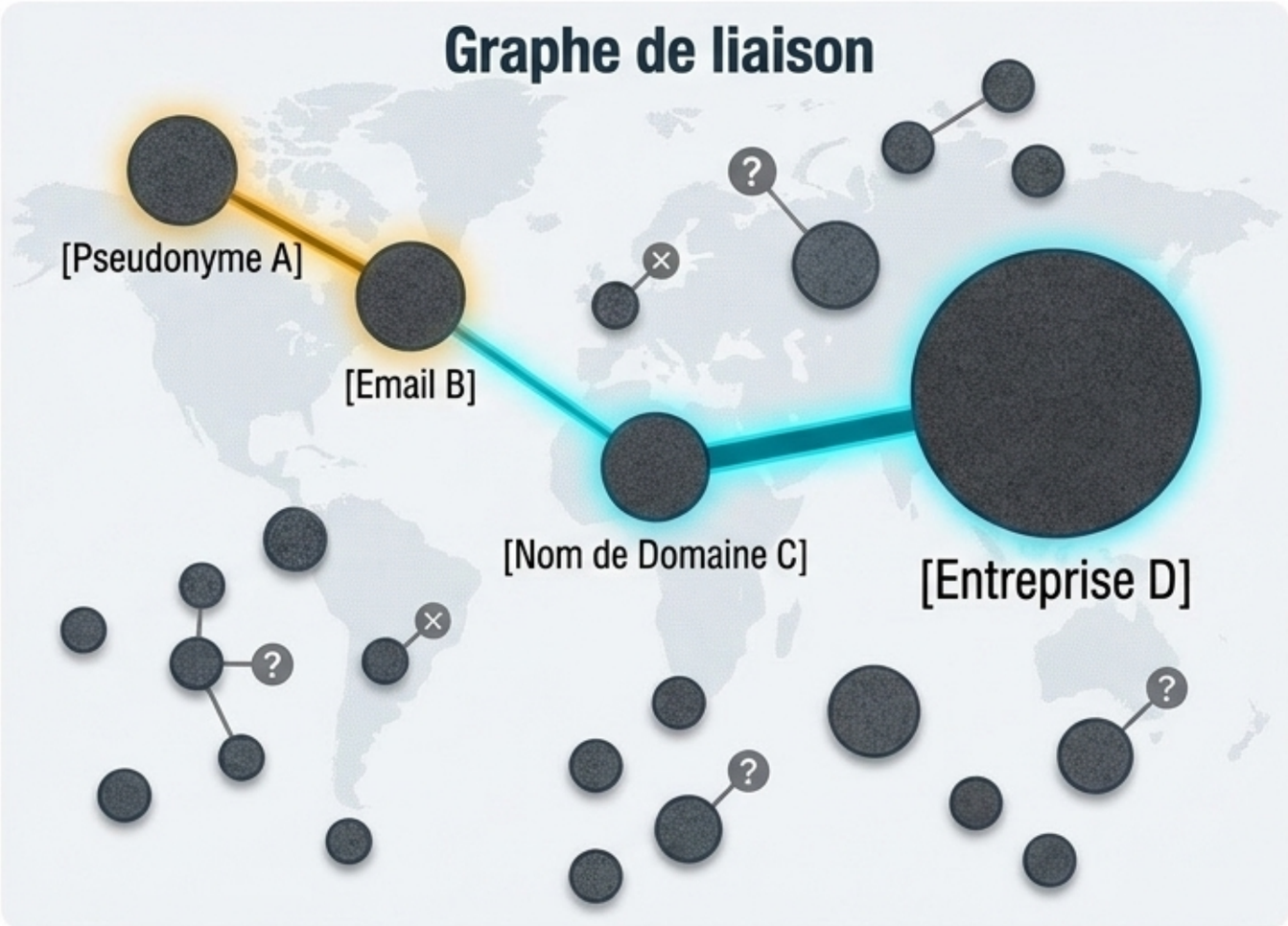
Une investigation produit rarement une preuve spectaculaire immédiate. Elle repose sur l’accumulation et la mise en relation de petits éléments (adresses, dates, formulations).

OSINT (Open Source Intelligence)

L’exploitation méthodique d’informations publiquement accessibles.

L’Enjeu

Séparer le signal du bruit dans un océan de données numériques pour identifier la véritable source d’une menace ou d’une fraude.



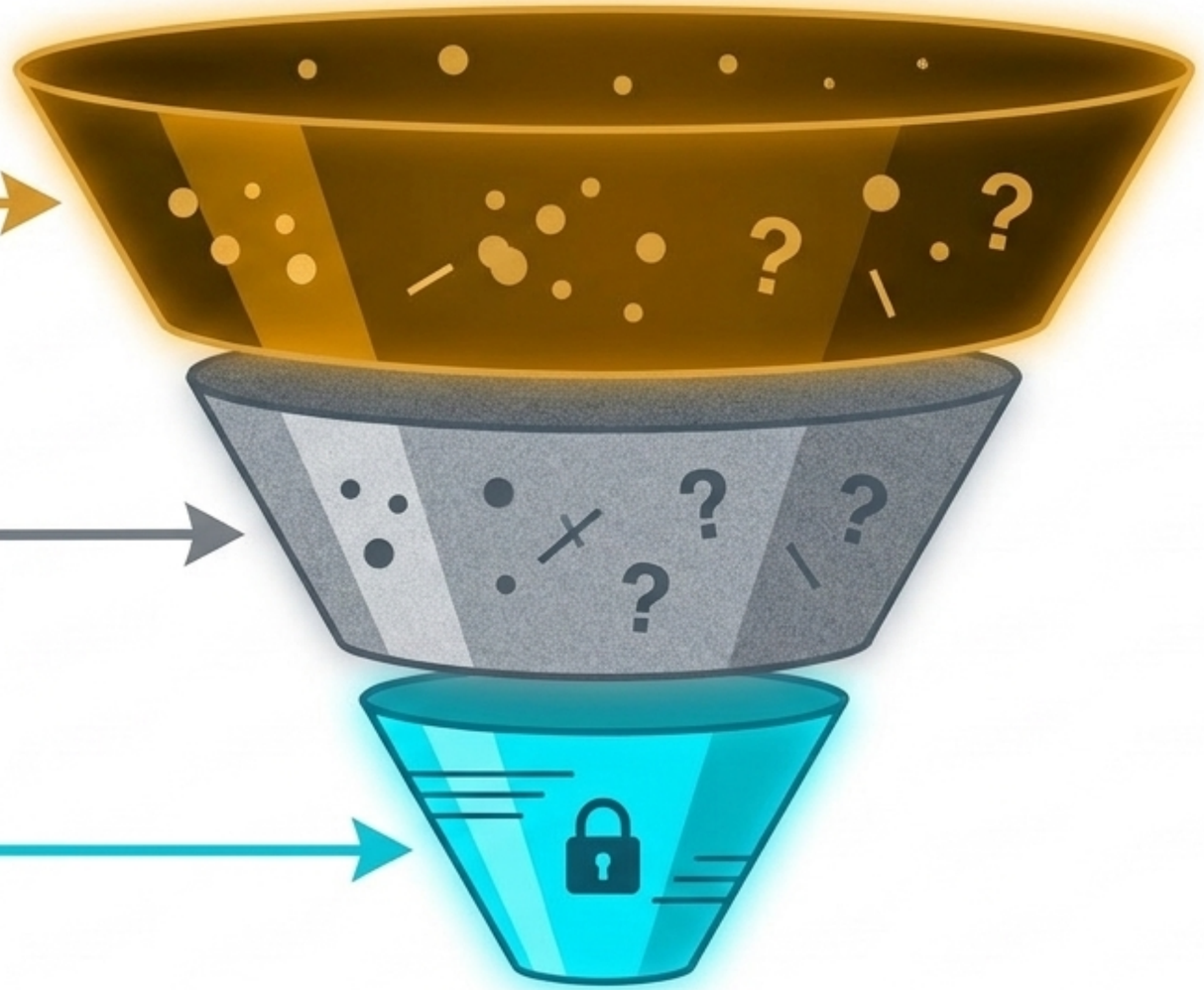
Le Processus de Vérification de l’Information

Ne jamais confondre Information disponible et Preuve.

Niveau 1 : Donnée Brute (Le Bruit)
Ex: Deux pseudonymes similaires ou Une rumeur très partagée. Risque élevé d’usurpation ou de falsification.

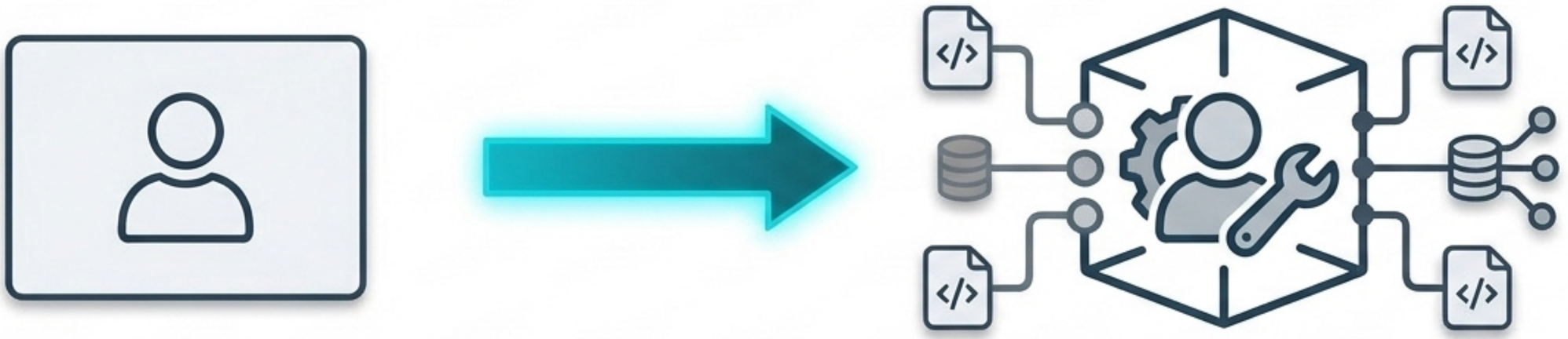
Niveau 2 : Recoupement (La Source)
Ex: Qui a produit l’information ? Dans quel contexte ? Recherche de corroboration indépendante.

Niveau 3 : Fait Établi (La Preuve)
L’information devient un indice qualifié, rigoureusement documenté et conservé pour soutenir un éventuel litige.



Pilier 3 : Formation à l’Informatique

Comprendre la technologie pour reprendre le contrôle.



Utilisateur Passif

Créateur d’Outils

Pourquoi coder ?

La programmation n’est pas une fin en soi. C’est un outil pragmatique pour résoudre des problèmes spécifiques d’investigation et d’analyse.

Automatisation

Remplacer une tâche répétitive (ex: vérifier 1000 liens ou extraire des données) par un script personnalisé.

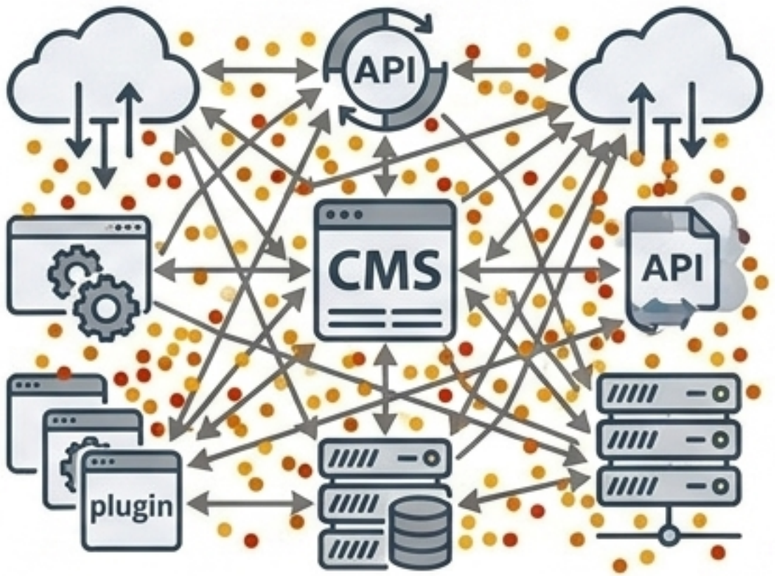
Indépendance

Ne plus dépendre exclusivement des boîtes noires logicielles commerciales. Comprendre son environnement permet de mieux le sécuriser.

Cybersécurité par la Simplification

Le progrès numérique n’est pas l’accumulation aveugle de technologies.

Le Système Obèse



Le Coût de la Complexité

Chaque dépendance externe (plugin, script tiers, service cloud) allonge la chaîne de vulnérabilité et crée une nouvelle surface d’attaque.

Le Système Lean / Local First

La Philosophie Pacta (Local First)

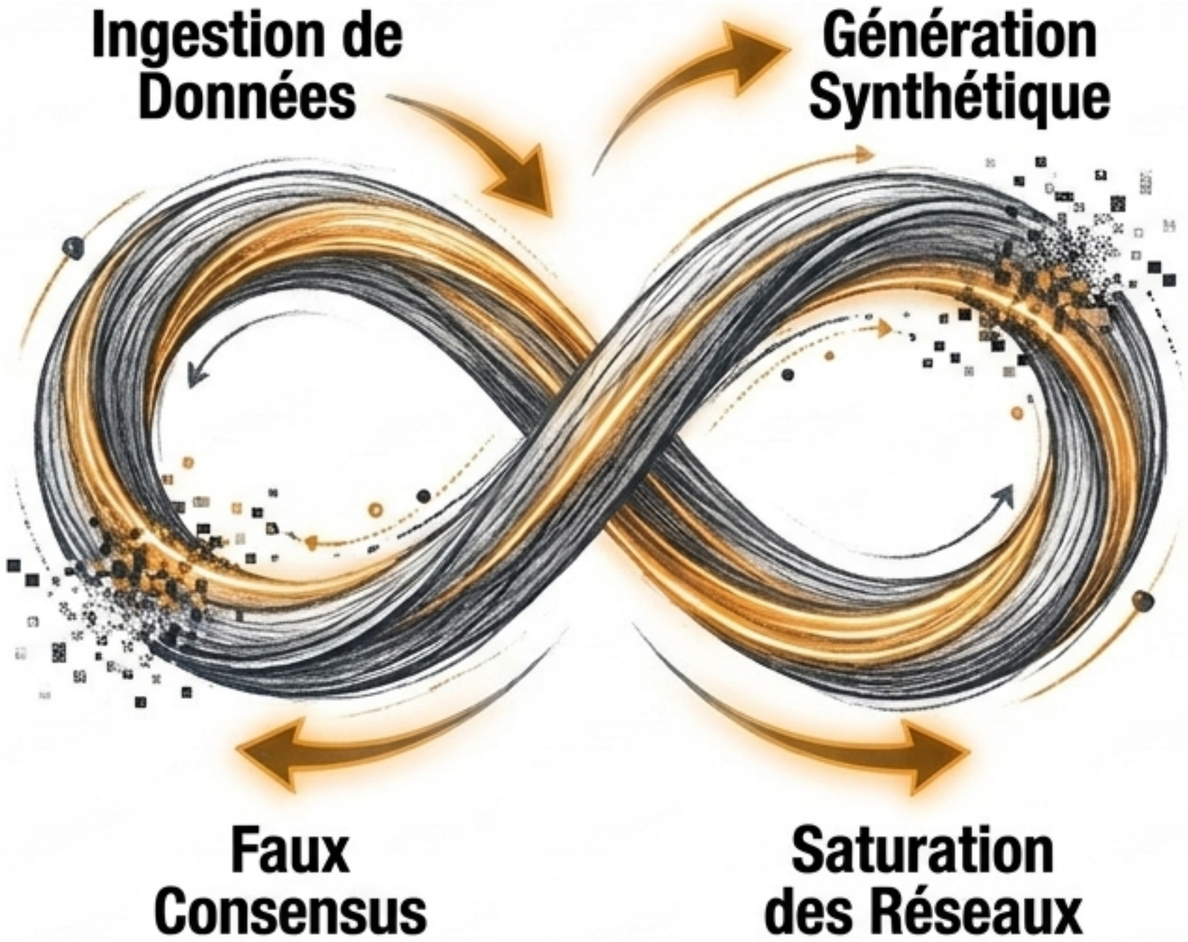
Conserver la technologie quand elle apporte une valeur réelle, mais supprimer la complexité inutile. Parfois, un programme local stable est infiniment plus sûr qu’une architecture cloud fragmentée.

Le Défi de l’Intelligence Artificielle

La nouvelle crise de confiance numérique.

La Menace : Production Industrielle

Production industrielle de l’illusion. Une fausse information répétée 100 fois par des IA 100 fois par des IA donne l’illusion d’un consensus factuel.



La Réponse : Culture de l’Enquête

Renforcer radicalement la culture de l’enquête. L’apparence parfaite d’un document ou d’une voix n’est plus une garantie. Identifier la source originelle, vérifier le contexte, et systématiser le doute.

L’Écosystème Global : Les 4 Laboratoires Pacta

Une vision transversale de l’indépendance numérique.

Pacta Cyber Lab (PROTÉGER) Analyse des risques, investigation numérique, et facteur humain.	**Pacta COBOL Lab (PÉRENNISER)** Stabilité, systèmes durables, et approche Local First.
Pacta Industry Lab (RELIER) La réalité physique de l’informatique (électronique, infrastructures, données vérifiées).	**Artopraxia (DÉCONNECTER)** Préserver l’autonomie humaine par la pratique manuelle et artistique, hors des écrans.

Gagner en Maîtrise, Réduire les Dépendances

Une nouvelle conception de la sécurité numérique.

OBSERVER l'environnement technologique et le comportement humain.

- **VÉRIFIER** systématiquement l'information à la source, surtout face à l'IA.
  - **PROTÉGER** par la sensibilisation et la réduction des surfaces d'attaque.
    - **COMPRENDRE** la technologie par la formation ciblée pour ne plus la subir.
      - **DÉCONNECTER** pour conserver sa liberté d'action hors du monde numérique.

Prêt à renforcer votre pare-feu mental et protéger vos données ?

Alain STEVENS - Pacta.com - Pacta Labs