



• ATELIER 45 MIN

Cybersécurité & IA

IA

Sécuriser le cabinet et ses données
données

Alexis Graef

Rapporteur général du Congrès

Président section IFEC Alsace

Expert-comptable à Strasbourg

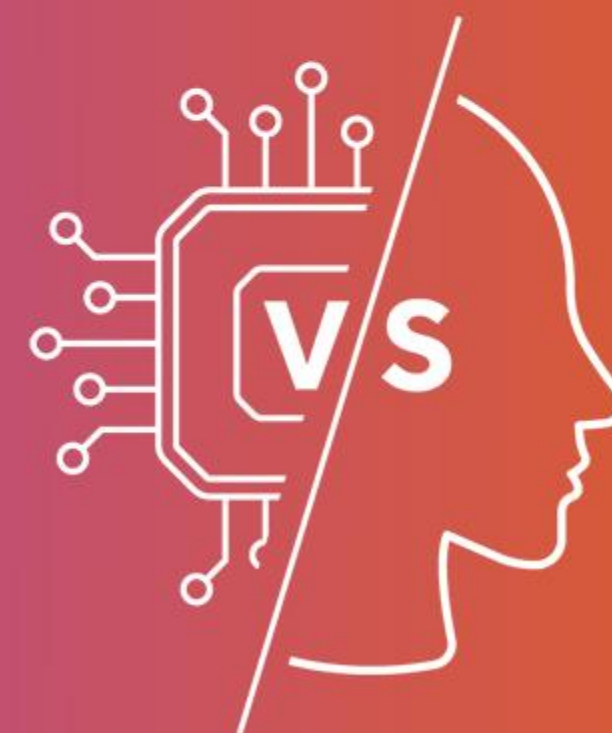
Pierre Dos Santos

Fondateur SOC Networks

Spécialiste cybersécurité Intégration

Intégration IA souveraine

CONGRÈS
IFEC
REIMS
○○○ 2026 ○○○



DÉFINITION

Shadow AI

L'IA utilisée hors de tout cadre défini par le cabinet.

Sans politique. Sans traçabilité.

Posées cette semaine, dans des cabinets



Clarisse, sur ChatGPT

« Relis ce mail et corrige les fautes »

→ mail client nominatif, collé tel quel



Thomas, sur Claude

« M. Dupont veut céder sa holding : quel traitement fiscal pour la plus-value ? »

→ nom du client anonymisé + montage patrimonial



Karim, sur Gemini

« Rends ce mail plus professionnel »

→ échanges clients confidentiels



Alice, sur ChatGPT

« Ordonne ces tâches selon les échéances fiscales »

→ portefeuille clients + échéances

Des usages utiles et déjà quotidiens mais **sans charte, sans directive, hors de tout contrôle du cabinet.**



CONGRÈS
IFEC
REIMS
000 2026 000

UNE QUESTION SIMPLE

Imagineriez-vous vos collaborateurs envoyer les liasses fiscales, fiscales, les déclarations de TVA ou les bilans de vos clients... clients... **depuis leur mail personnel ?**

Non. Jamais. Tout ce qui engage le cabinet passe par les outils gérés par le cabinet et leurs prestataires .

Avec l'IA, c'est pourtant exactement ce qui se passe aujourd'hui.

Et c'est plus dangereux encore : on ne lui confie pas seulement des données, on lui demande de **produire**.

Quatre régimes s'appliquent

01 Secret professionnel

Toute donnée confiée par un client est couverte, y compris si elle transite par une IA.

02 RGPD

Responsabilité du traitement : base légale obligatoire, droits des personnes garantis.

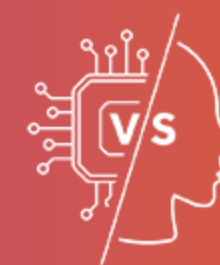
03 Règlement européen sur l'IA

L'employeur doit garantir que ses équipes maîtrisent les outils d'IA qu'elles utilisent.

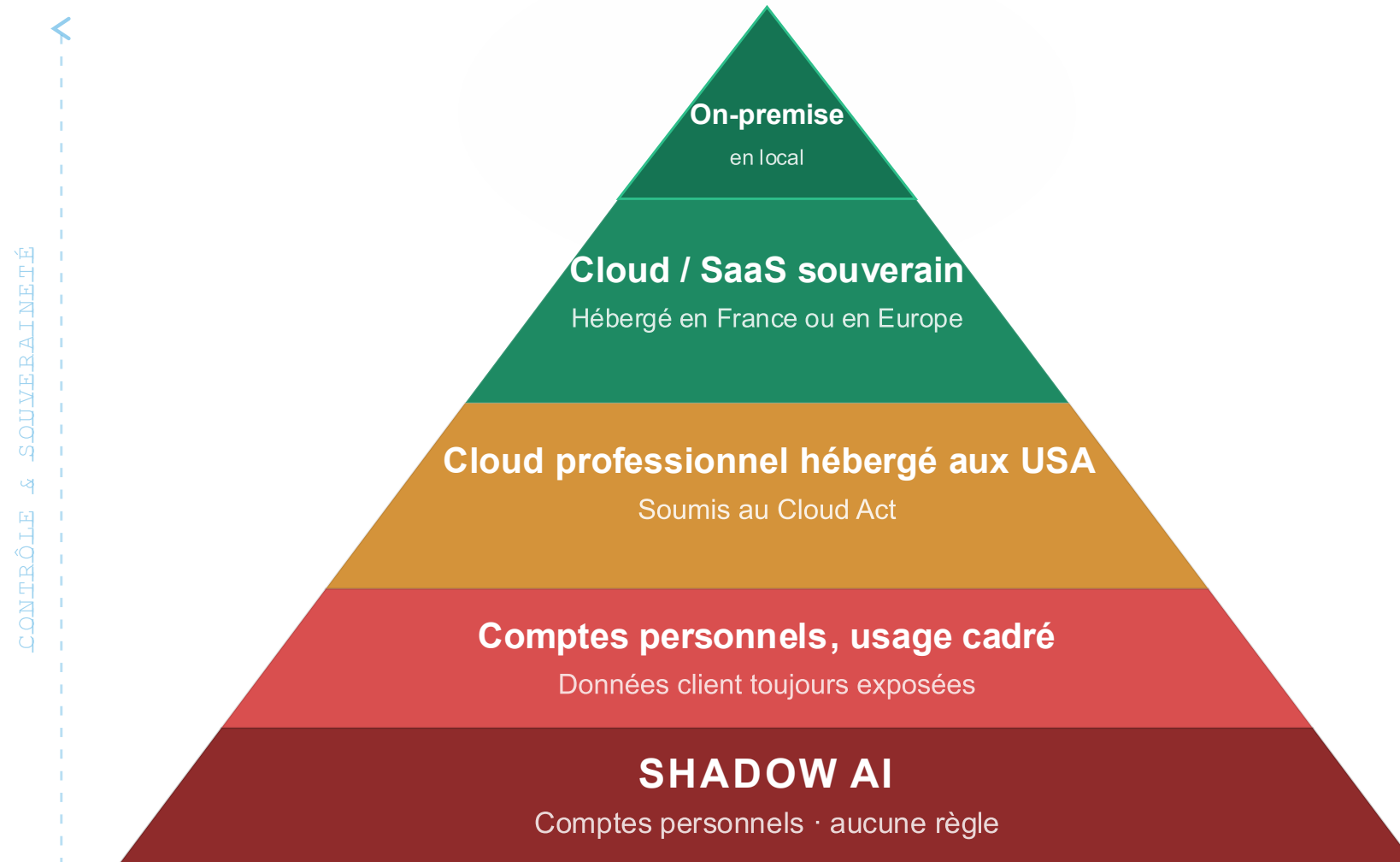
04 Responsabilité professionnelle

Le cabinet répond des outils utilisés par ses collaborateurs dans le cadre de leurs de leurs missions.

Sans politique IA, le cabinet répond d'usages qu'il ne connaît pas.



Trois niveaux de souveraineté



- **CONFORME**

Données confiées à un fournisseur européen, hébergées en Europe. RGPD respecté, secret professionnel préservé.

- **RISQUE · JURIDICTION ÉTRANGÈRE**

Un fournisseur américain peut être contraint de livrer vos données et de ne pas vous le dire.

- **ILLÉGAL**

Confier des données client à un compte personnel, c'est violer le secret professionnel.



L'IA au service des hackers



Utilisateur



Une technologie commune avec une intention
différente.



Attaquant

armé d'IA
d'IA



Des attaques dopées à l'IA

01 Hameçonnage parfait

Mails indiscernables, rédigés dans le style exact de vos interlocuteurs.

02 Voix et style clonés

Un appel d'un client ou d'un prestataire, potentiellement fabriqué.

03 Logiciels qui se réécrivent

Un antivirus travaille comme un contrôle sur liste. L'IA produit une variante inédite à chaque attaque : elle n'est sur n'est sur aucune liste.

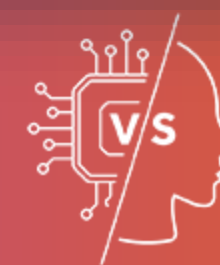
EXEMPLE CONCRET

La messagerie du cabinet, retournée contre ses clients

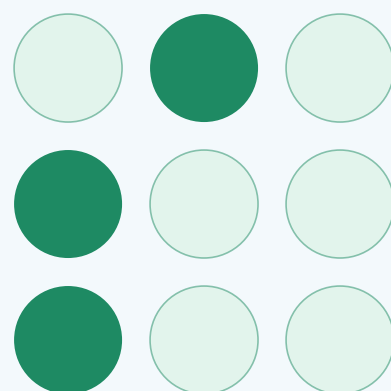
Un cabinet se fait voler ses accès mail. Les attaquants observent trois semaines, puis ciblent deux clients seulement, les plus gros gros encours.

Depuis la vraie adresse, dans le style exact du collaborateur : nouveau RIB pour les prochains règlements. Dans la signature, le numéro de téléphone a été remplacé.

Le client qui appelle pour vérifier... tombe sur le fraudeur.



L'antivirus fait sa part. Pas tout.

TEMPS 1**Ce qu'il fait bien**

L'antivirus et le pare-feu restent **indispensables** : ils arrêtent l'essentiel des menaces connues.

+

TEMPS 2**Ce qu'il faut ajouter**

Face à une menace inédite et sophistiquée, il est essentiel de **surveiller les comportements**. Détection continue des anomalies sur le réseau, réaction dès le premier signal pour réduire la fenêtre d'exposition.

PLAN D'ACTION

Par où commencer

Le réflexe n°1

~~Interdire et bannir l'IA~~

01

Équiper

Une solution IA respectant le secret professionnel, au service du cabinet



02

Cadrer

Une charte : qui utilise l'outil, pour quelles données, données.



03

Protéger

Une supervision cyber : détecter les comportements anormaux avant les dégâts.

Reprenez le contrôle de votre IA.



CONGRÈS
**IFEC
REIMS**
000 2026 000



L'IA est déjà dans votre cabinet. La question, c'est question, c'est de savoir **qui pilote.**

VENEZ NOUS VOIR

Stand SOC Networks

Pierre Dos Santos

06 63 42 78 49 · pds@soc-networks.com

Solution IA souveraine et sécurisée pour les cabinets

SOC NETWORKS × IFEC REIMS 2026

