Cybersécurité & IA 2026
PMEs loin d'être prêtes

Cybersécurité & IA

PME : un retard structurel, à l'échelle européenne

Cybersécurité PME

Une prise de conscience réelle des risques, mais encore trop peu d'actions structurantes

Cyberattaques

Exposition massive, préparation réelle très faible

72%

des organisations constatent une hausse des risques cyber

43%

des entreprises européennes ont subi au moins une cyberattaque
en 2024–2025

<40%

des PME ont réalisé une analyse de risques cyber formalisée

<30%

des PME ont identifié et classifié leurs données sensibles

<20%

réalisent des exercices ou simulations de crise cyber

Les entreprises sont attaquées, mais elles ne savent pas vraiment ce qu'elles protègent, ni comment réagir.

(World Economic Forum, cybersecurity outlook 2025)

(UK Cyber Security Breaches Survey 2025, tendances UE similaires sur ENISA et Eurostat)

(France : Cybermalveillance.gouv.fr 2025 / Suisse : NCSC)

Accumulation d'outils, pas de vision globale

65%

des PME disposent d'au moins une solution de cybersécurité

(antivirus, firewall, sauvegarde, EDR…)

67%

des PME n'ont pas de stratégie cyber pleinement opérationnelle

≈50%

des incidents réussis exploitent des failles déjà connues ou non patchées

<35%

ont une architecture cyber cohérente et pilotée

(outils intégrés, procédures, responsabilités claires)

<25%

disposent d'un SOC ou d'une supervision continue, même externalisée

Les entreprises achètent de la sécurité. Elles ne la gouvernent pas.

(UK Cyber Security Breaches Survey 2025, tendances UE similaires sur ENISA et Eurostat)
(France : Cybermalveillance.gouv.fr 2025 / Suisse : NCSC)

Gestion de crise, le grand absent

65-70%
des TPE–PME n'ont aucune procédure de réaction, de plan d'urgence

49%
Des PME déclarent ne pas savoir gérer une cyberattaque

+50%
des cas, la détection de l'incident est externe
(client, partenaire, journaliste, autorité)

<20%
ont testé leur plan au moins une fois
(exercice de crise, table-top, simulation)

<25%
ont désigné une cellule de crise avec rôles et responsabilités clairs
(IT, juridique, direction, communication)

30%
des PME disposent d'un plan de gestion de crise cyber formalisé

Quand l'incident survient, l'organisation improvise.

IT for Business
Digital Switzerland
(France : Cybermalveillance.gouv.fr 2025 / Suisse : NCSC)

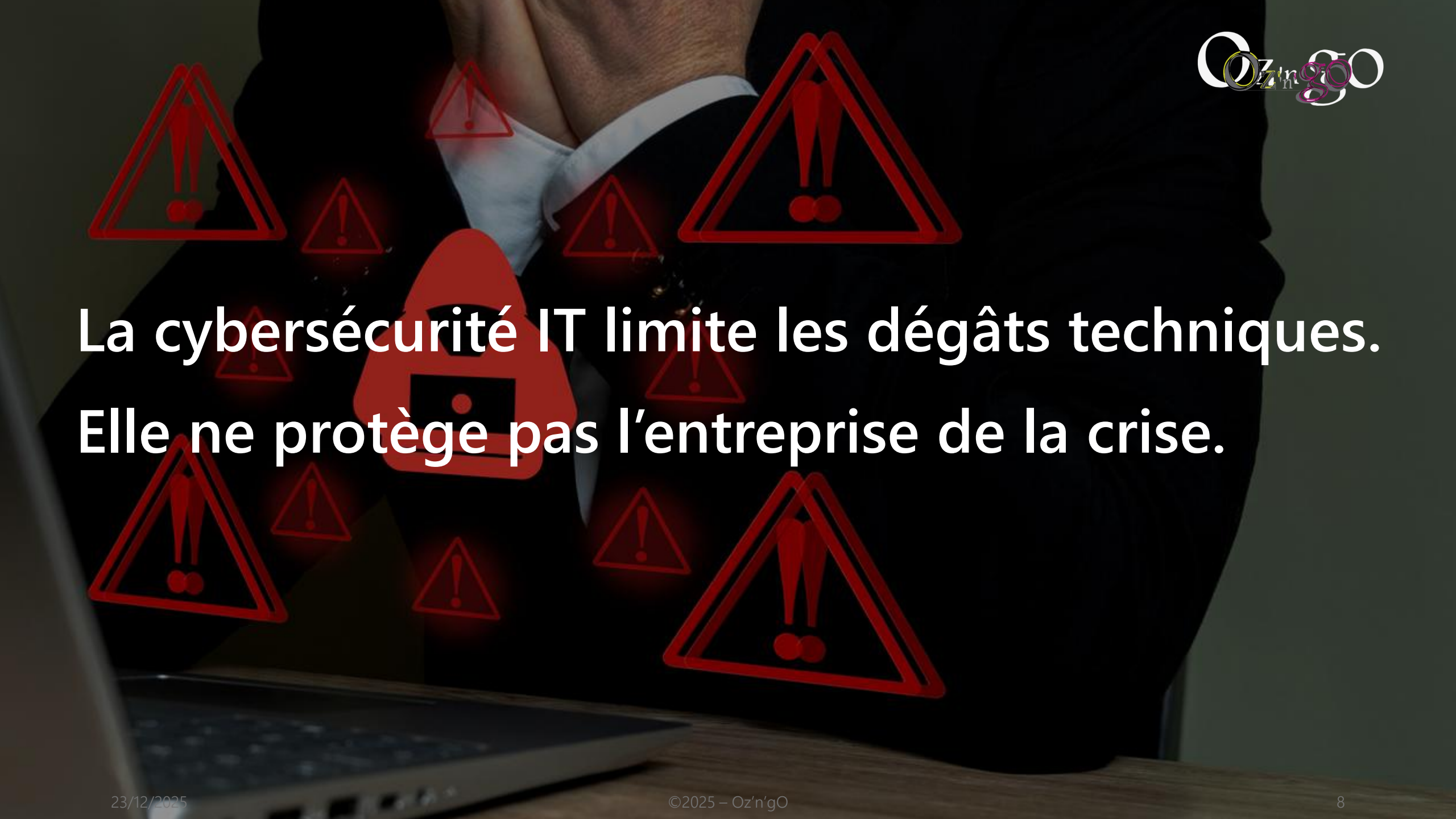
Communication de Crise, le chaînon vital manquant

Dans la majorité des PME

- aucun porte-parole clairement désigné et préparé
- aucune articulation claire entre IT, juridique et communication
- aucun canal de communication sécurisé identifié en amont
- aucune préparation aux réseaux sociaux et à la pression médiatique
  (messages pour les équipes, les clients et fournisseurs, les autorités, les journalistes)

- silence
- messages contradictoires
- communication tardive ou improvisée
- perte de crédibilité

Les entreprises sécurisent leurs systèmes, pas leur parole.



La cybersécurité IT limite les dégâts techniques.

Elle ne protège pas l’entreprise de la crise.

Intelligence Artificielle

Une adoption progressive

sans compréhension réelle

de ce qu'est l'IA ni de ses risques

Adoption de l'IA en Europe

Une croissance marquée

20%

Des entreprises européennes utilisent l'IA

+30%

sont des PME entre 50 et 250 personnes

50%

sont des entreprises de +250 personnes

17%

sont des TPE de moins de 50 personnes

+18%

Des PME de 10 à +250 personnes utilisent l'IA

88%

prévoient d'augmenter leurs investissements IA dans les 12 prochains mois.

34%

Des PME de 10 à +250 personnes utilisent l'IA

Diffusion rapide de l'IA mais asymétrique, en fonction de la stratégie, la structure et la taille du pays mais aussi le niveau de connaissance des dirigeants à l'IA et les capacités d'intégration opération-nelle. Le Danemark illustre cette dynamique (+40 %)

Eurostat, AI in Enterprises, dec 2025
OpinionWay, Février 2025
Conseil Fédéral, nov 2025

Usage de l'IA en Europe par secteur d'activité

L'IA avance d'abord dans les secteurs structurés par la donnée et la régulation. Ailleurs, le retard n'est pas technique, mais organisationnel et culturel.

92%
Banques, Finance, Assurance

+62%
Information & Communication

+40%
Recherche scientifique & technique

25%
Immobilier

+20%
Hôtellerie & Tourisme

20%
Services administratifs et d'assistance

≈18%
Commodities

≈17%
Industrie

Technologies IA utilisées en Europe

surtout NLP/LLM et la création de contenu Audiovisuel

12%
Text mining

9.5%
Images, vidéos & audio

9%
Textes & Codes

+7%
Transcription

+5%
Automatisation de flux & processus

5%
Machine Learning

L'IA est, en général, largement utilisée, mais peu comprise. Les organisations des autres secteurs privilégient les usages les plus simples, au détriment des capacités analytiques et décision-nelles.

Banques, Finance & Assurance

Text mining (70-80%)
Workflows or décision assistée (60-70%)
Machine learning/Deep learning (80%)

Eurostat, , *AI in Enterprise* dec 2025
SPGlobal, article Oct. 2025
EY Parthenon survey, sep 2025
European Banking Authority (EBA), 2025

L'IA, pour quel usage en Europe
surtout Marketing/Vente et process admin/business

35%
Marketing & Vente

31%
Processus Admin & Business

+23%
Comptabilité & gestion financière

21%
Processus de production

Entreprises de +250 personnes
Majoritairement cybersécurité (+47%) et dans les processus business/admin (+43%)

Entreprises entre 10 et 250 personnes
Majoritairement Marketing & Sales (36%/34%) et les process business/admin (35%/28%)

Banques, Finance & Assurance
Majoritairement Cybersécurité (85%) et les process finance/compta (75%), suivi des process de production (70%) et des business/admin (60%)

L'IA est d'abord utilisée là où le ROI est immédiat, et pour la sécurité. On cherche le rendement rapide et sécurisé sur des usages qui exposent le plus aux dérives narratives, réputationnelles et humaines.

Eurostat, , *AI in Enterprise* dec 2025
SPGlobal, article Oct. 2025
EY Parthenon survey, sep 2025
European Banking Authority (EBA), 2025

Connaissance de l'IA par les chefs d'entreprise

4 réalités

1 L'IA est connue mais mal comprise

58%

des dirigeants de PME-TPE considèrent l'IA comme un enjeu de survie

32% l'utilisent vraiment

<1/3 savent expliquer précisément ce qu'est l'IA et ses usages

2 L'IA est largement réduite à la génération/analyse de contenu

70-80%

des usages déclarés de l'IA concernent des NLP/ LLM génératifs

rédaction, résumé, traduction, chatbots, analyse de textes

3 Les modèles analytiques sont peu identifiés

<20%

des dirigeants savent distinguer IA générative et IA analytique décisionnelle

(scoring, détection d'anomalies, pricing, risk modelling)

4 Familiarisation ≠ maîtrise

57%

des professionnels européens déclarent se former à l'IA

L'IA est utilisée en n'en comprenant qu'une partie, confondant outils, modèles et risques.

Bpifrance
McKinsey, State of AI, nov 2025
Eurostat, AI in Enterprise, dec 2025

Une perception des risques IA largement sous-estimée

11-15%

des dirigeants considèrent aujourd'hui l'IA comme un risque stratégique

68%

des dirigeants continuent de voir l'IA avant tout comme une opportunité

Malgré l'augmentation documentée des incidents

-51%

des organisations utilisant l'IA ont vécu au moins 1 conséquence négative

(erreurs, hallucinations, décisions biaisées, atteintes réputationnelles)

<30%

des entreprises européennes ont mis en place une gouvernance IA

(politiques d'usage, contrôle, audit, gestion de crise IA)

Les risques sont réels, mesurés, déjà vécus. La prise de conscience reste largement insuffisante.

McKinsey, State of AI, nov 2025
ISACA / Almost a third of European businesses lack formal AI policies (2025)
(EY European AI Barometer jul 2025)

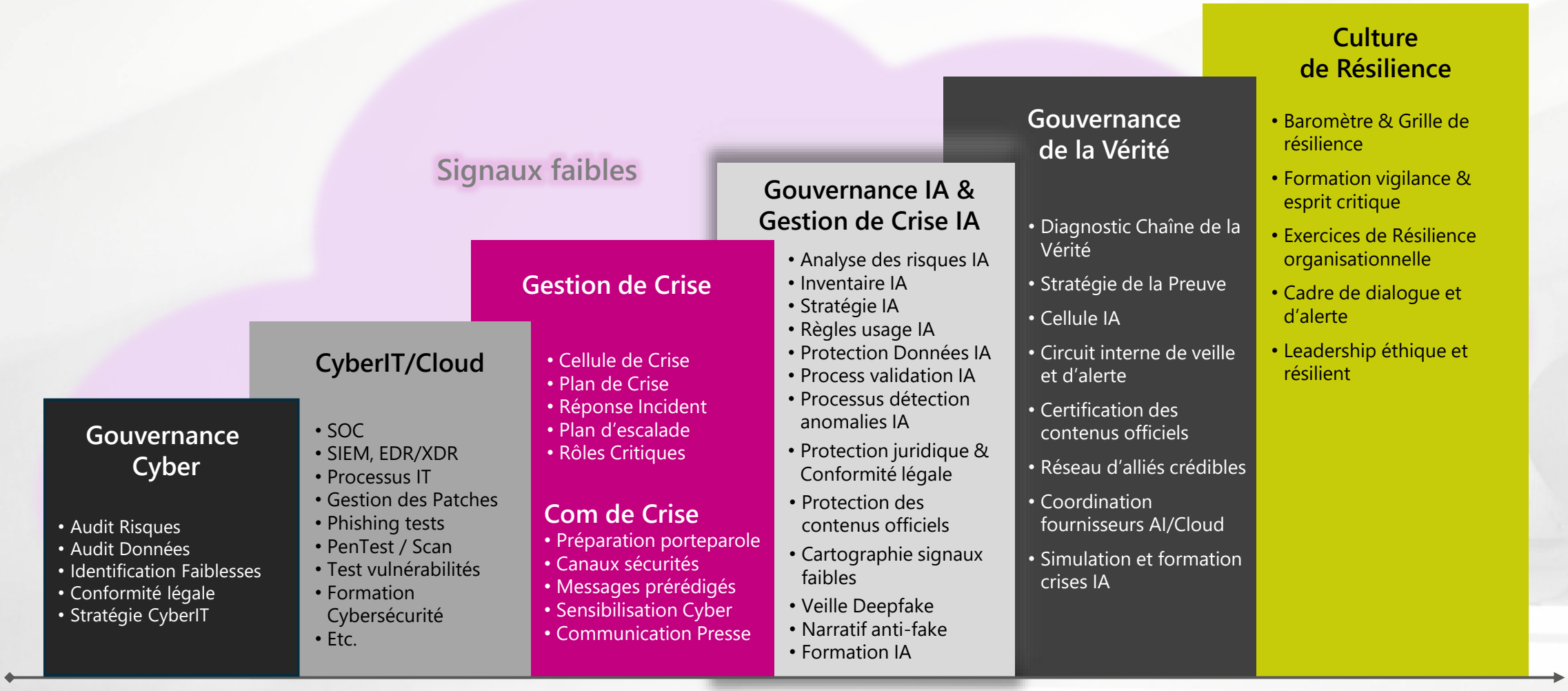
Le problème n’est pas ce que fait l’IA.

C’est ce qu’on lui laisse décider.

Inquiet ?

C’est bon signe.
Vous allez dans la bonne direction.

Le périmètre idéal de la cybersécurité à l'ère IA



LES 4 ANGLES **MORTS**
que la gouvernance techno-centrée ne couvre pas

Décisions altérées =
1ère cible du hacker

Culture, cohésion et partage
vos meilleures défenses

Les **bonnes personnes** doivent voir les **bonnes anomalies** au **bon moment**

Votre bouclier Vérité
en cas de crise IA

LE NOUVEAU RISQUE EST INVISIBLE

Avec la pression interne comme surface d'attaque

- Sous pression, les équipes deviennent plus manipulables, moins vigilantes.
- L'IA amplifie exactement les signaux qui déstabilisent : confusion, surcharge, doute.

Les hackers exploitent ce que votre management fragilise

À L'ÈRE DE L'IA,
LA SEULE DÉFENSE DURABLE

c'est la cohésion humaine.

Maryse Rebillot

contact@ozngo.com

+41 77 533 77 67

www.ozngo.com