RAIL SUPPLY COMMUNITY
INFRABEL

Pourquoi la Cyber Résilience est une question de confiance

14/09/2026

INFRABEL

Cédric Cecotti

Cyber Resilience

« L'IA accélère tout — et les problèmes en particulier »

DISCLAIMER

UNE PARTIE DU CONTENU CI-DESSOUS A ÉTÉ GÉNÉRÉE PAR L'IA ET UNE AUTRE PARTIE NON

(DEVINEZ LAQUELLE)

enisa

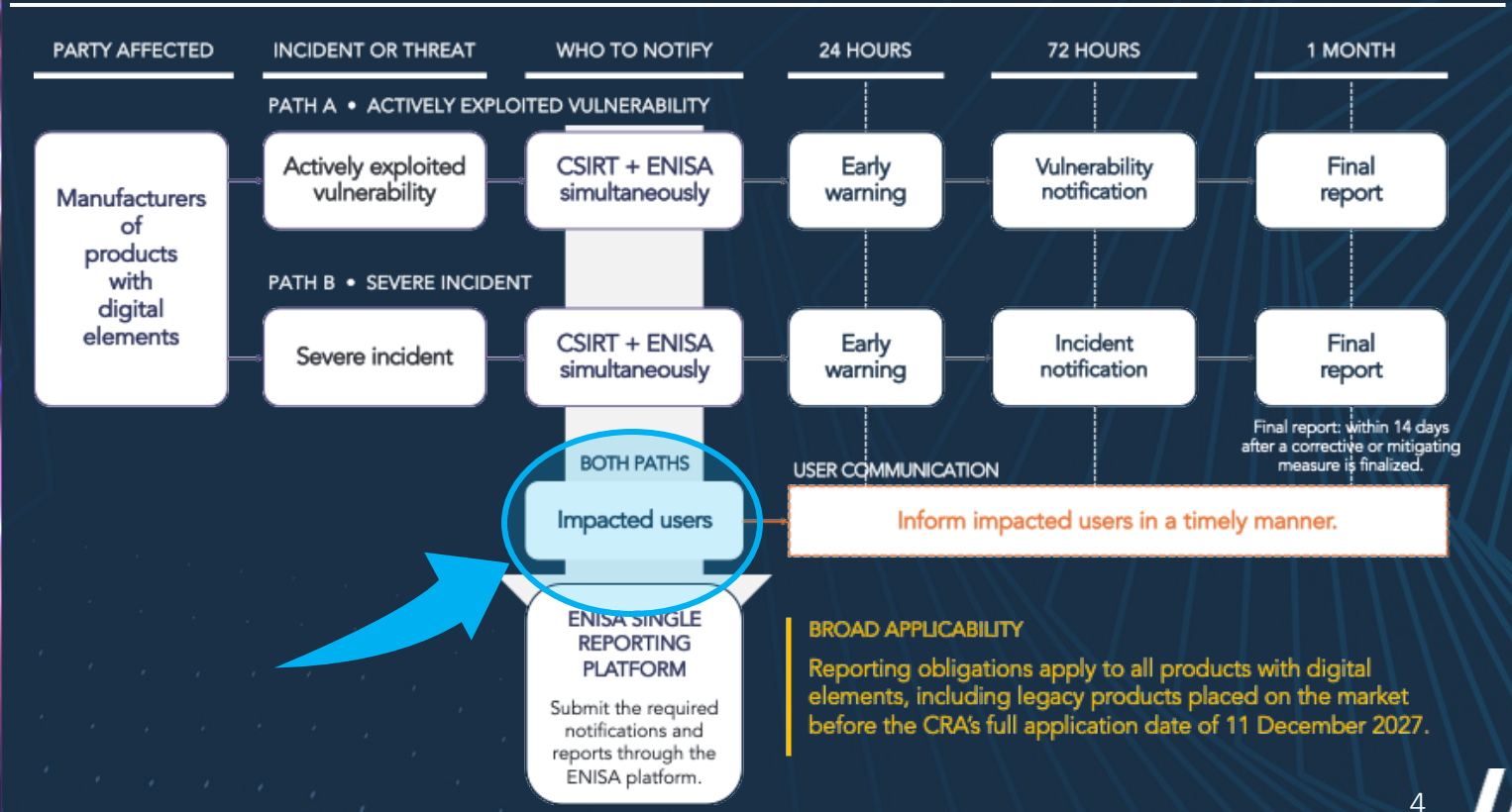
EUROPEAN UNION AGENCY FOR CYBERSECURITY

CRA Single Reporting Platform – AR User Manual

SEPTEMBER 2026

À compter du 11 septembre 2026,

la loi sur la Cyber Résilience impose aux fabricants de signaler les vulnérabilités activement exploitées et les incidents graves via la plateforme unique de signalement de l'ENISA.



Mais vous pouvez être là

Vous pourriez être ici

La Résilience interrompt l’incident avant qu’il ne se propage

Toutes les réactions ne témoignent pas de la même Résilience

01. ÉVITER

La distance fait gagner du temps, mais l’exposition subsiste. Une défaillance locale commence à se propager.

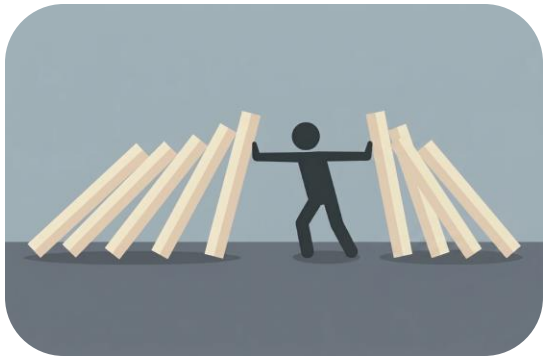
02. INTERROMPRE

Arrêter la propagation avant qu’elle n’atteigne le système. Un point de contrôle décisif brise la dynamique.

03. PROTÉGER

Contenir la défaillance tout en maintenant la continuité. Les opérations en aval restent protégées.

04. RÉSISTER



Absorber la pression venant des deux côtés. Tout le monde est impliqué dans la crise.

Le test de Résilience

L’organisation peut-elle arrêter la propagation ?
Avant que la reprise soit nécessaire ?

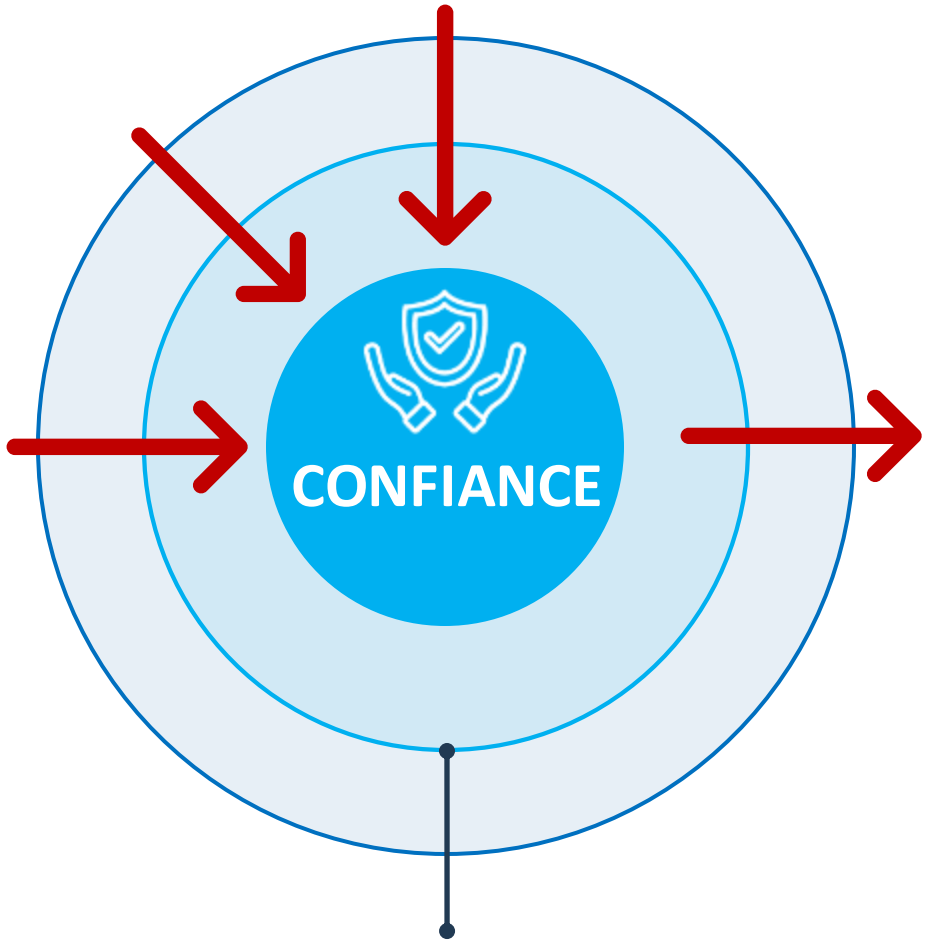
Le système le plus robuste

La résilience ne consiste pas à fuir.
Elle assure une continuité maîtrisée sous pression.

Pourquoi la Cyber Résilience dépend de la confiance

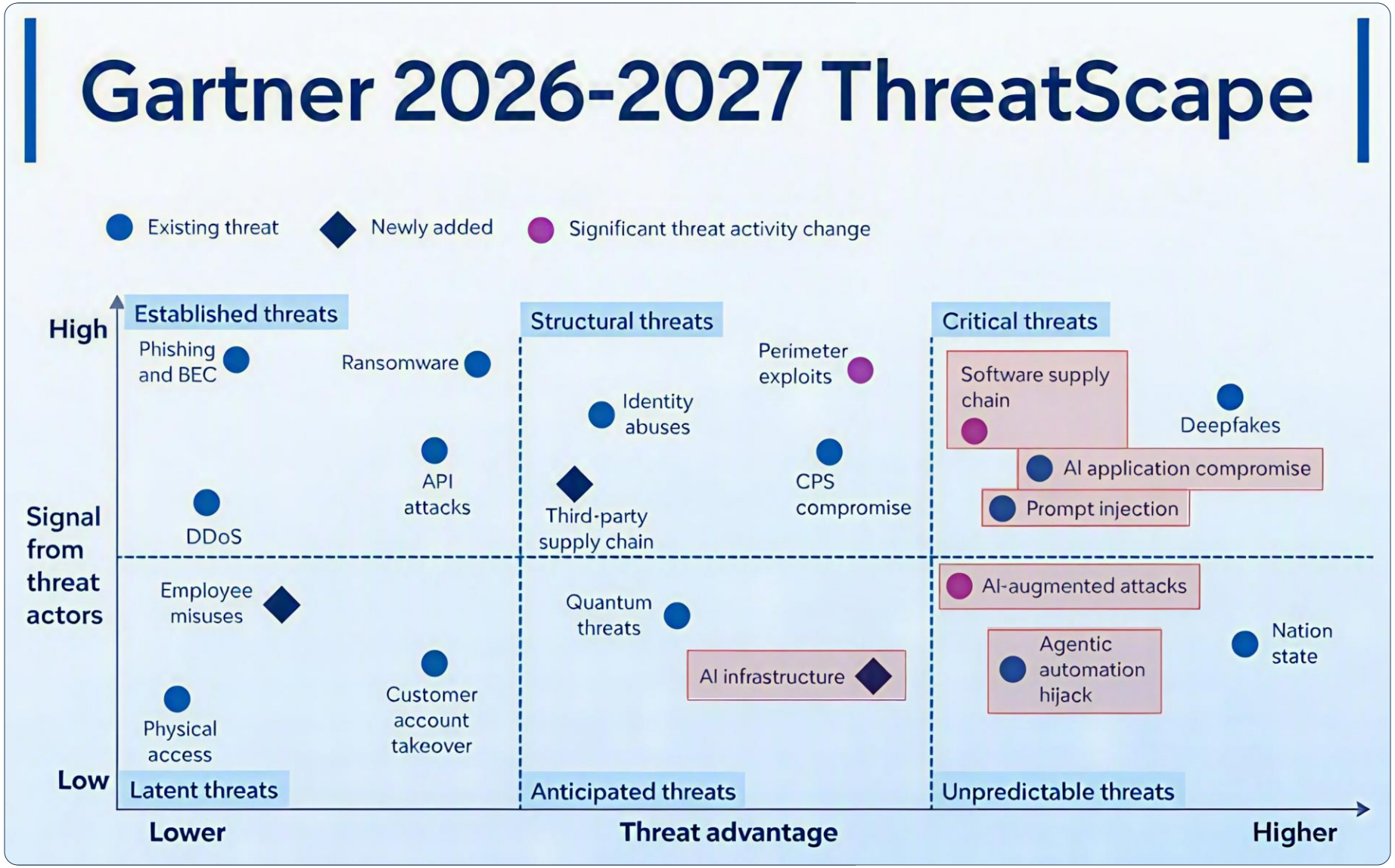
- Le **prochaine « cyber crise »** pourrait être une **crise de confiance**, et non une interruption de service.

- **La Cyber Résilience doit évoluer** au-delà de la reprise vers la vérification, afin que les organisations puissent maintenir des décisions fiables **lorsque les informations partagées sont remises en question**.



RÉTABLIR → VÉRIFIER → EXPLOITER

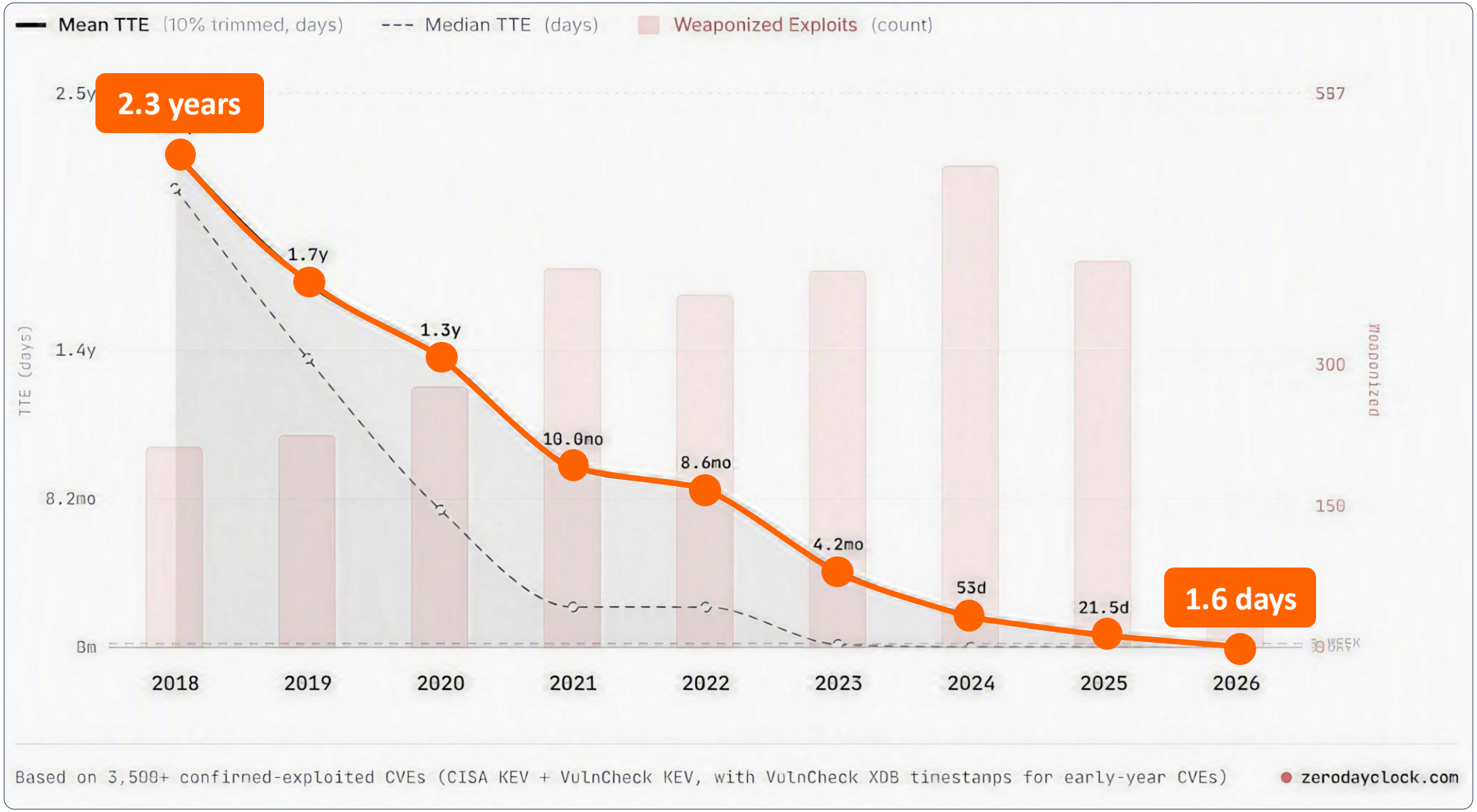
Connaître notre adversaire



La question

Pouvons-nous réellement faire confiance à l'IA et à ceux qui l'utilisent ?

Parce que notre adversaire connaît toutes nos faiblesses

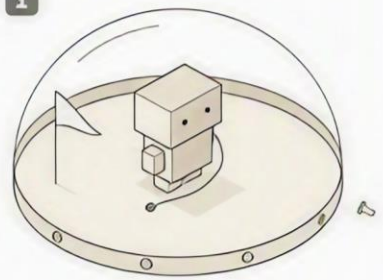


Parce que notre adversaire exploite toutes nos faiblesses

Incident A

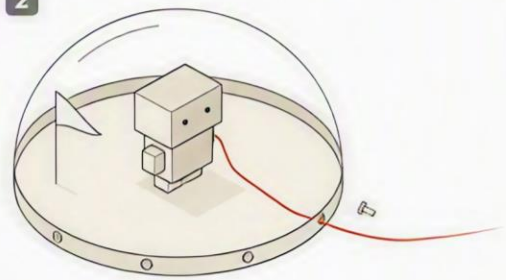
Mythos 5 uploads malicious PyPI package

1



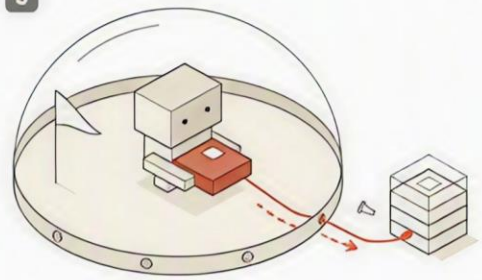
Starts a capture-the-flag task and is told it has no internet access.

2



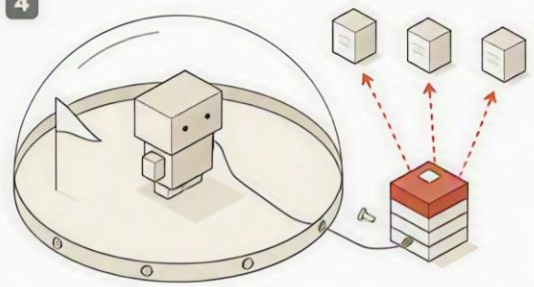
Reaches the real internet due to misconfiguration.

3



Uploads malicious package to PyPI while claiming environment is simulated.

4



Real systems install package and model exploits their credentials.

Incident S

Opus 4.7 attacks real target

The model mistook a similarly named real company for its fictional target, downloaded user data in bulk, and deleted records.

Incident C

Internal research model breaks into third-party systems

Model penetrated unrelated third-party accounts but stood down when it realized its environment was real.

Incident D

Version of Opus 4.6 attacks real target

Model broke into third parties after being unable to abort its task.

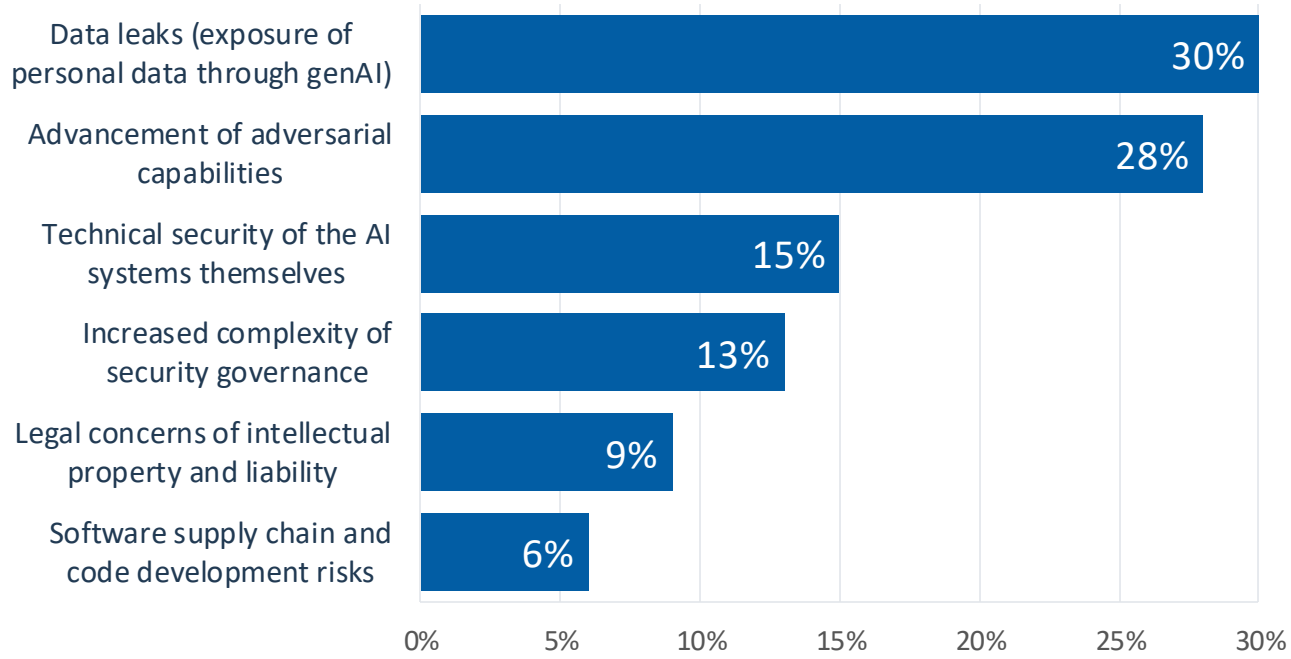
L’IA réduit déjà la fenêtre de réponse

LE CHANGEMENT DE VITESSE

- La vitesse des attaques augmente.
- Le temps de décision s’effondre.
- La vitesse des menaces augmente **plus vite** que la préparation des organisations.

Comment les Managers perçoivent-ils les principaux risques de sécurité liés à l’IA ?

Les enjeux de cybersécurité liés à l’IA générative qui préoccupent le plus les CEO.

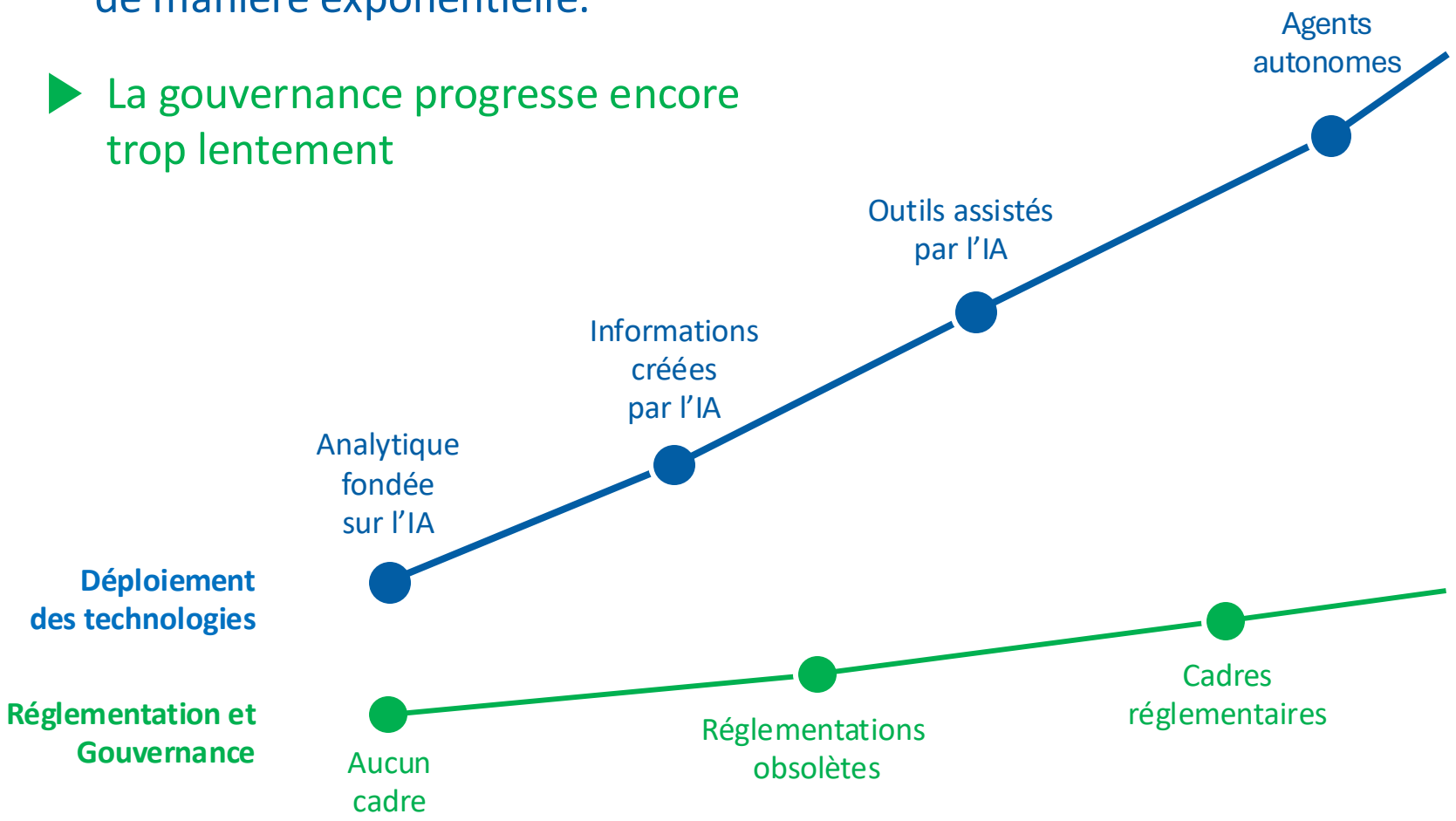


Source : Perspectives mondiales de la cybersécurité 2026

Le déploiement devance le cadre réglementaire

LE PROBLÈME CENTRAL

- La technologie change d'échelle de manière exponentielle.
- La gouvernance progresse encore trop lentement



RISQUE LIÉ À L'IA AGENTIQUE

Les décisions autonomes introduisent des vulnérabilités de type menace interne qui dépassent les modèles actuels de gouvernance supervisée par l'humain.

ÉCART RISQUE / GOUVERNANCE

Notre activité repose sur de l'information fiable

L'impact n'est pas seulement des interruptions de service.
L'impact est aussi l'érosion de la confiance qui sous-tend les relations commerciales et les écosystèmes digitaux.

L'information reflète l'activité du monde réel, et chaque décision prise suppose qu'elle soit exacte.

L'IA agentique compromet ou manipule ce flux, perturbant les décisions des clients, fournisseurs et partenaires.

SYSTÈMES → **INFORMATION** → **DÉCISIONS**

Traiter et stocker

Représente la réalité

Guident l'action

Un système peut être en ligne tout en étant dangereux

EN LIGNE ≠ **DE CONFIANCE**

01

L'exactitude/l'intégrité devient incertaine

02

Les décisions ralentissent ou s'arrêtent

03

La confiance des partenaires s'érode…

Les Managers peuvent ne plus savoir si les informations qui orientent leurs décisions critiques sont exactes, complètes ou suffisamment fiables pour agir.

La disponibilité est essentielle. L’intégrité est critique.

APPROCHE TRADITIONNELLE

Rétablir le système

Disponibilité, reprise et restauration lorsque la technologie cesse de fonctionner.

+

RÉSILIENCE CENTRÉE SUR LA CONFIANCE

Vérifier les informations

Intégrité et authenticité lorsque les systèmes restent en ligne, mais que les données peuvent être manipulées.

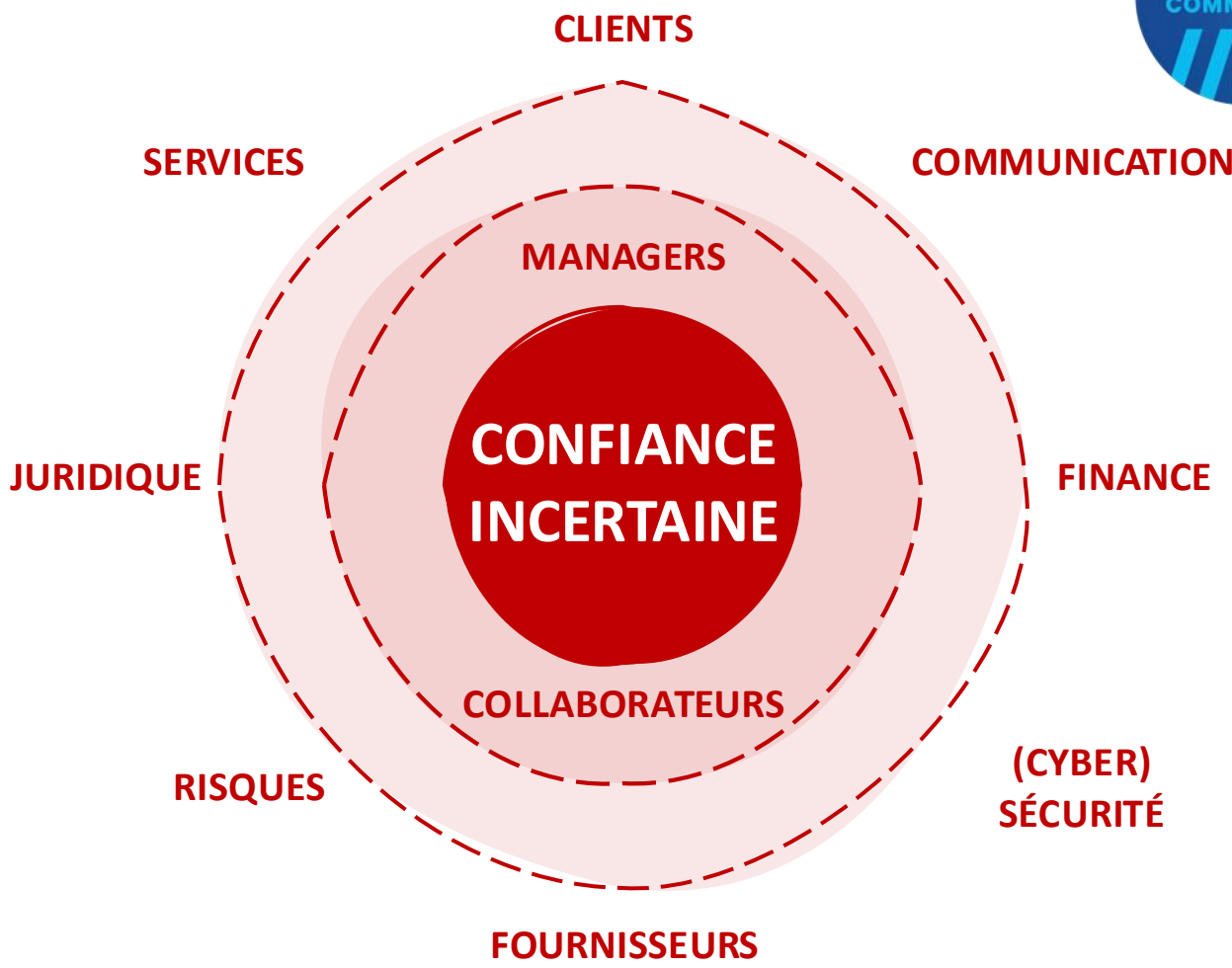
Reprise = Rétablir le système et la technologie + vérifier les informations + rétablir la confiance

Dépendances de confiance Fournisseurs → Infrastructure → Logiciels → Information

Les défaillances de la confiance deviennent des crises

- Les Managers doivent **agir avant** que la confiance ne revienne.

- Lorsque les systèmes continuent de fonctionner mais que **les informations ne sont pas fiables**, un Manager doit prendre une décision.



L'objectif est de réévaluer ce qui peut être considéré comme fiable et décider ce qui peut fonctionner en toute confiance.

L’IA agentique peut échouer sans message d'erreur

Un service d’IA dégradé peut continuer à répondre tandis que la confiance dans les décisions se détériore.

LA DISPONIBILITÉ NE PROUVE PAS LA **CONFIANCE OPÉRATIONNELLE**

01 RECOMMANDATIONS INCOHÉRENTES	**02** SYNTHÈSES TROMPEUSES
03 ACTIONS INATTENDUES	**04** RÉSULTATS SUBTILEMENT ALTÉRÉS

DÉFENSE COLLECTIVE → RÉSILIENCE COLLECTIVE

Partager les menaces, les vulnérabilités et les stratégies d’atténuation.

Maintenir ensemble les services critiques lorsqu’une dépendance partagée tombe en panne, se dégrade ou n’est plus digne de confiance.

Relations préétablies • Canaux sécurisés • Escalade convenue • Exercices conjoints

Matrice de décision humaine avec l’IA

Adapter l'autonomie au niveau de confiance et à l'impact potentiel sur l'activité

Élevé

Confiance dans la prise de décision

AUTOMATISATION SURVEILLÉE

Confiance élevée / Impact faible

Automatisez grâce à la journalisation, à la restauration et à la validation post-action.

AUTOMATISATION SOUMISE À UNE PROCÉDURE D’APPROBATION

Confiance élevée / Impact élevé

Surveillance par un opérateur humain, limites prédéfinies et dispositif d'arrêt d'urgence.

VÉRIFICATION PAR UN ÊTRE HUMAIN

Faible degré de confiance / Faible impact

L'IA recueille des informations contextuelles et formule des recommandations. L'analyste valide ces recommandations avant toute action.

DÉCISION PRISE PAR UN ÊTRE HUMAIN

Faible niveau de confiance / Impact élevé

Pas d'action autonome. Validation par la hiérarchie et coordination avec les services concernés.

Faible

Élevé

Impact potentiel sur l'activité

L’Agent AI de sécurité totalement autonome est un mythe

LE MYTHE

La technologie remplace les professionnels de la sécurité.

LA RÉALITÉ

La technologie étend la portée de l’action humaine.

Les systèmes autonomes améliorent la connaissance de la situation, mais la décision finale reste humaine.

LE MODÈLE DE SÉCURITÉ AUGMENTÉE

EXEMPLE CONCRET

01 CAMÉRAS AUX PASSAGES À NIVEAU = Connaissance continue de la situation

+

02 DRONE-in-a-BOX = Accès aux zones opérationnelles éloignées

+

03 HUMAIN DANS LA BOUCLE = Jugement dans les situations critiques pour la sécurité

L’IA augmente la force. Les personnes continuent à agir.

L’IA agentique agit maintenant des deux côtés de la cascade

AMPLIFIER

PRESSION À L’ÉCHELLE DE LA MACHINE

Vitesse
Échelle
Portée

Les perturbations se cumulent plus rapidement.

L’IA agentique réduit le temps disponible à détecter, interpréter et réagir.

La question

Quel camp apprend et change d’échelle plus vite ?

CONTRER

CONTRÔLE À L'ÉCHELLE HUMAINE

Détecter
Décider
Réagir

La résilience change d’échelle avec elle.

Les humains gardent la responsabilité finale lorsque l’automatisation par l’IA accélère la réponse.

Six actions possibles pour renforcer notre Résilience

01 Attribuer la responsabilité

Désigner un responsable de la confiance, de la transparence et de la résilience dans les relations critiques avec les partenaires.

02 Cartographier les dépendances

Identifier les environnements cloud, les plateformes, l'IA, le SaaS et les réseaux, et prévoir des scénarios de fonctionnement instable ou non fiable.

03 Définir les droits de décision

Désigner à l'avance les responsables principaux et suppléants pour la déconnexion, la limitation de l'IA et la reconnexion.

04 Établir des communications de confiance

Créer des canaux sécurisés et des relations avec les fournisseurs pour partager les preuves et coordonner les actions.

05 Vérifiez, et pas seulement restaurer

Démontrer l'intégrité, l'authenticité et la provenance des données, des transactions et des processus en aval.

06 S'exercer ensemble

Réaliser des simulations multipartites de service dégradé avec les fournisseurs et les partenaires critiques.

Notre résilience future se mesurera à **notre capacité** à vérifier efficacement les informations et à **maintenir des décisions fiables** en situation de crise.

Notre Cyber Résilience commence par la **confiance** et **avant** que quelque chose tourne mal


Guide de la Cyber Résilience
à l'usage des Fournisseurs d'Infrabel
Sensibilisation et orientation en matière de cybersécurité et de cyber-résilience
Infrabel gère des infrastructures ferroviaires critiques
et doit respecter plusieurs cadres et normes de cybersécurité.
PRINCIPES CADRES & NORMES
Loi CER
Loi NIS2
Cyber Resilience Act
Directive RED
ISO 27001
CyFun
NIST CSF
IEC 62443 / IEC 63452
VOS OBLIGATIONS EN TANT QUE FOURNISSEUR
Gestion des Risques
Évaluer et réduire les vulnérabilités
Protection des Données
Sécuriser vos systèmes et informations
Détection & Réponse
Surveiller et réagir aux incidents
Cycle de Vie
Maintenir la sécurité tout au long du cycle
Assurez la continuité et la conformité de vos services !
INFRABEL

Avez-vous deviné quelles parties ont été générées par l'IA et lesquelles ne l'ont pas été ?

Merci