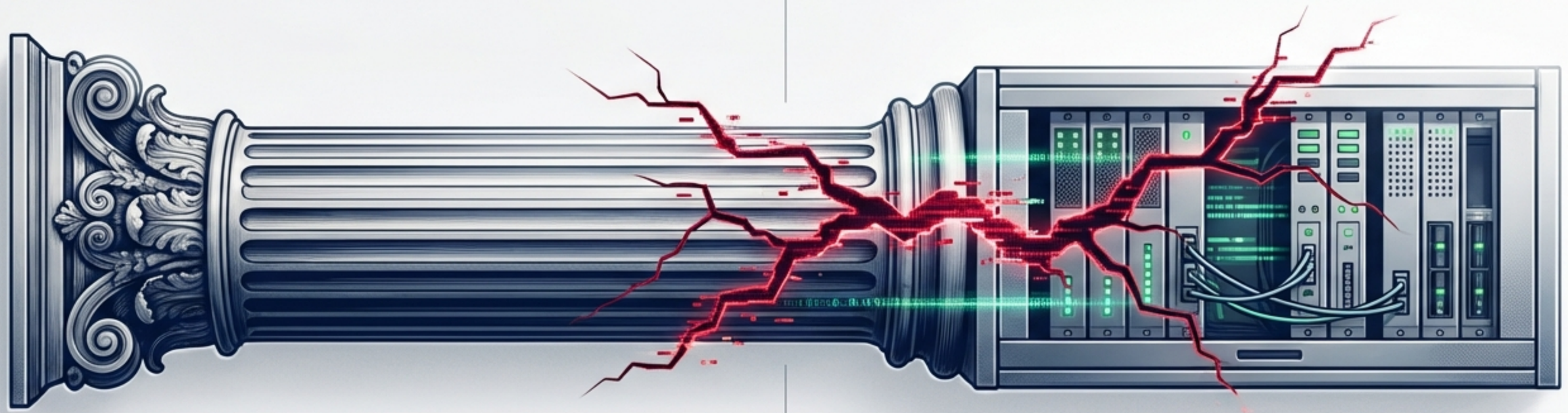
État de la Menace Cyber 2025

L'Ère de l'Industrialisation et de la Responsabilité

Analyse des dynamiques criminelles, impacts de la directive NIS2
et impératifs de résilience pour les décideurs français.



Rapport Stratégique – À l'attention du Comité Exécutif (COMEX)

Synthèse : Ce qu’il faut retenir en 2025

Explosion Volumétrique

+74%

d'attaques en 5 ans.
348 000 incidents recensés en 2024.
La menace est une certitude statistique.

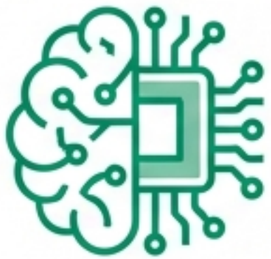
Bascule Géopolitique

Transition d’une cybercriminalité opportuniste vers une déstabilisation systémique et de l’espionnage stratégique post-JOP.

Le Choc Réglementaire (NIS2)

Fin de l'impunité. La responsabilité pénale et personnelle des membres du conseil d'administration est engagée.

L’Arme à Double Tranchant



L'IA générative industrialise les attaques (phishing parfait) mais devient indispensable pour la défense automatisée.

Une Menace Systémique et Industrialisée

Le modèle ‘Cybercrime-as-a-Service’ (CaaS) abaisse la barrière à l’entrée.

ESPIONNAGE

Vols de secrets industriels.
Cibles : Défense, Haute Tech.

EXTORSION

Rançongiciels et vol de données.
Modèle économique dominant.

DÉSTABILISATION

Sabotage et hacktivisme.
Nuisance à l’image et paralysie.

Coût estimé pour la France en 2025 : 100 milliards d’euros

Le Bilan des JOP 2024 : Un ‘Stress Test’ National

Le Succès Défensif

Aucune perturbation des épreuves sportives malgré une menace multipliée par 10.

La Réalité de la Menace

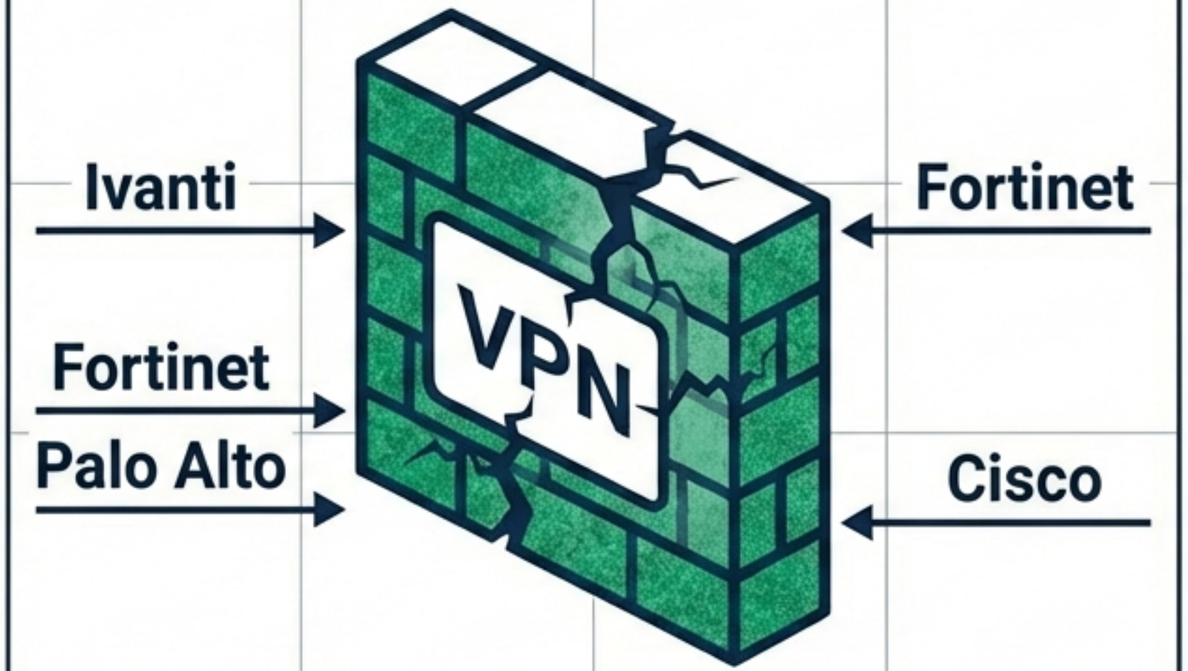
- **Déstabilisation massive** : Attaques DDoS intenses.
- **Hacktivisme** : 707 revendications en 2024 (Groupes pro-russes/pro-palestiniens).
- **Cas Concret** : Affaire POLADA (Agence antidopage).

Exfiltration de données médicales et campagne de désinformation (Fake News) par UNC1151.

Conclusion stratégique : La déstabilisation est désormais une arme de guerre hybride permanente.

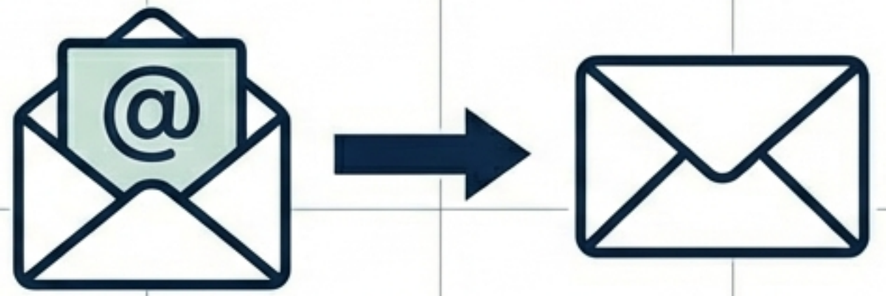
Les Portes d’Entrée : L’Effondrement du Périmètre

La Faillite du Edge



Exploitation de failles 'Zero-day' pour une intrusion profonde sans alerte.

L’IA Offensive



Phishing 2.0 : Messages contextuels générés par IA.

Deepfakes Audio/Vidéo

Secteur Privé : La Donnée comme Monnaie d'Échange

TÉLÉCOMS - Free (Oct 2024)

Fuite massive : 19 millions d'abonnés, IBANs inclus.

RETAIL - Kiabi (Jan 2025)

Credential Stuffing.
Fuite des IBAN de 20 000 clients.

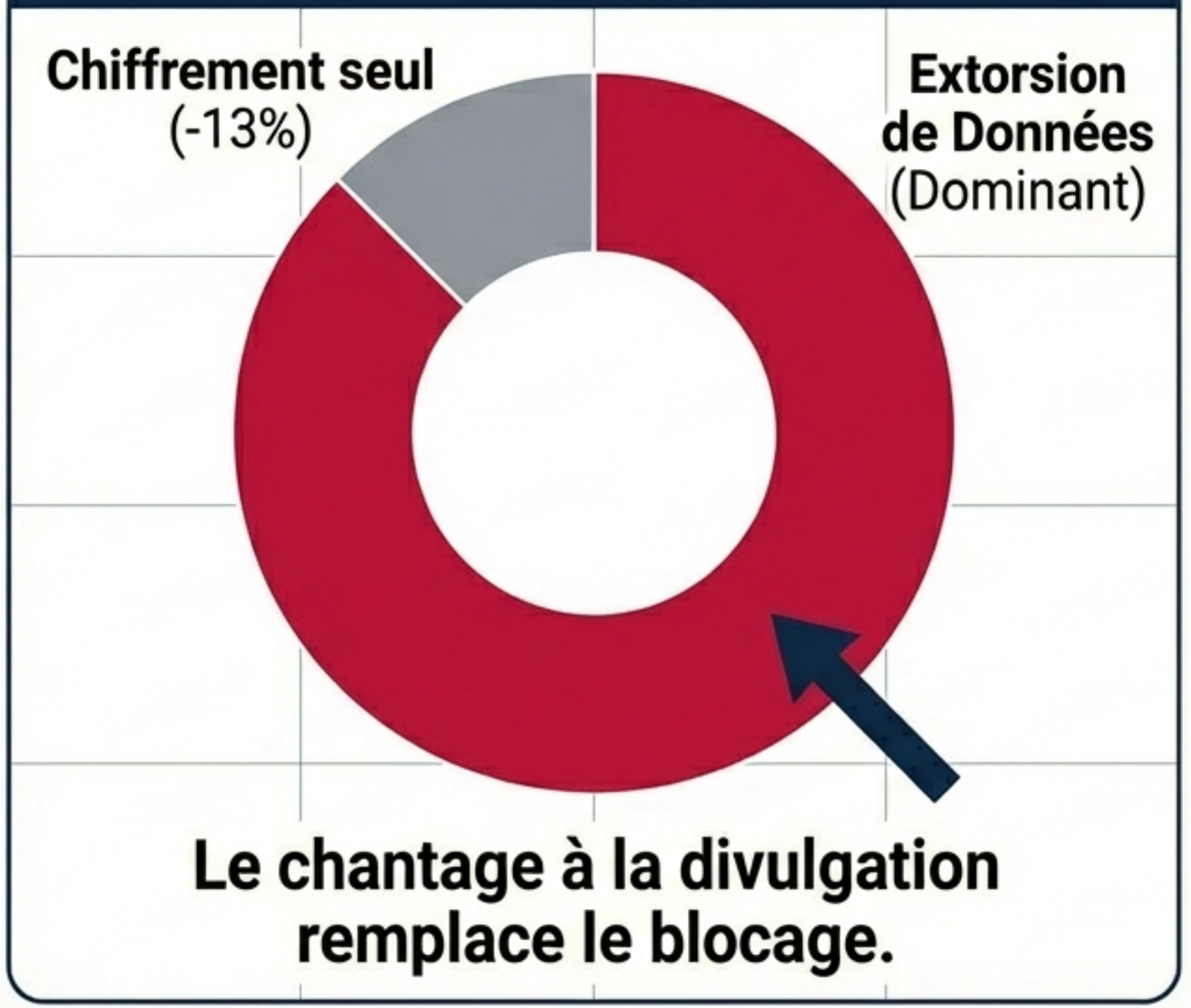
LOGISTIQUE - Chronopost (Jan 2025)

210 000 clients impactés.

SERVICES - Boulanger / Auchan

Séries de fuites de données clients.

Tendance



Le chantage à la divulgation remplace le blocage.

Secteur Public & Santé : L'Impact Sociétal

SANTÉ (Urgence Vitale)

10% des rançongiciels visent la santé.

CH Stell (Mars 2025) : Retour forcé aux procédures papier.

ADMINISTRATION (Donnée Sociale)

30% des attaques visent les administrations.

France Travail (43M personnes impactées).
Mairie de Poitiers (Paralysie état civil).

Les attaques sur le secteur public ne visent pas l'argent, mais la confiance des citoyens.

La Précarité Numérique des PME

77%

Des victimes sont des PME/TPE

60% des PME attaquées font faillite sous 18 mois.

Le déficit de maturité

25%
Gestion sécurité inexistante.

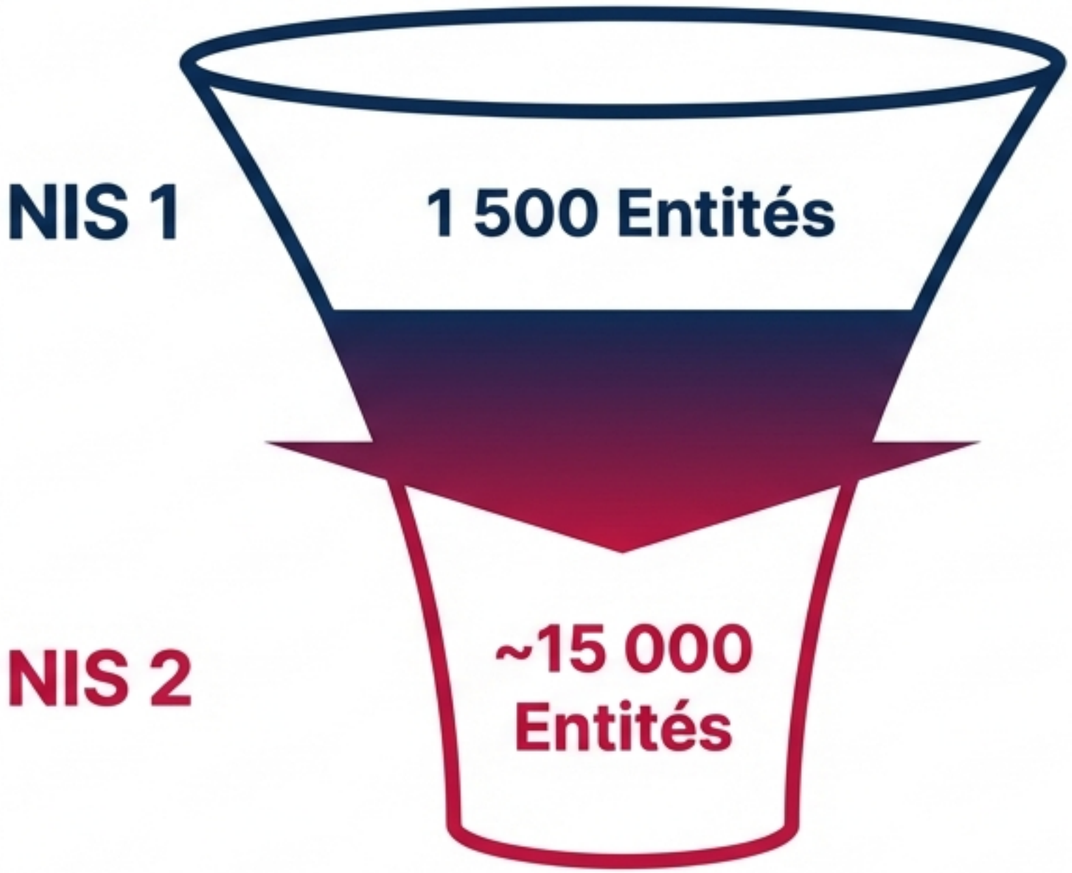
91%
Aucune assurance cyber.

77%
Budget annuel < 2 000 €.

Le tissu économique français est exposé sans filet de sécurité.

Le Choc Réglementaire : La Directive NIS2

De l’incitation à l’obligation de résultat.



Entités Essentielles (EE)	Entités Importantes (EI)
• Énergie • Transports • Banques • Santé • Eau • Infra Numérique.	• Agroalimentaire • Déchets • Fabrication • Recherche • Services Numériques.

Gouvernance : La Fin de l’Impunité

RESPONSABILITÉ PERSONNELLE

- Les dirigeants (COMEX/Board) sont personnellement responsables.
- Obligation de formation validée pour les instances dirigeantes.

SANCTIONS FINANCIÈRES

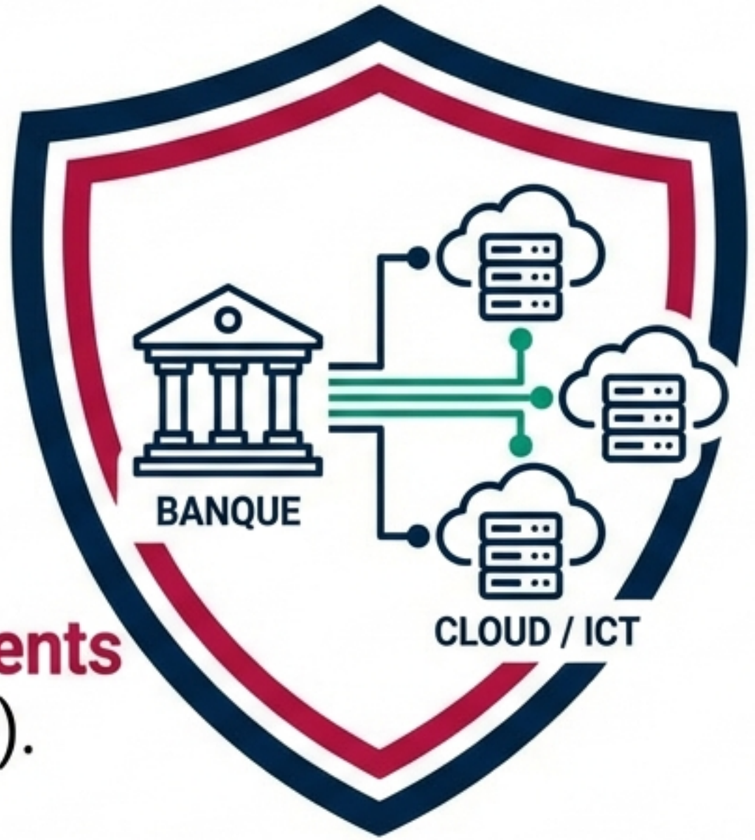
Jusqu’à 10 M€
ou 2% du CA mondial
Entités Essentielles

Jusqu’à 7 M€
ou 1,4% du CA mondial
Entités Importantes

Impératif : Notification des incidents majeurs sous 24 heures à l’ANSSI.

Focus Secteur Financier : La Résilience Opérationnelle (DORA)

En vigueur :
17 janvier 2025.



Risque Tiers :
Gestion stricte des prestataires ICT/Cloud.

Menace : Le secteur bancaire = **46% des incidents financiers** (Source: ENISA).

Obligation : **Tests de pénétration réguliers**.

Objectif : Garantir la survie des opérations en cas de crise systémique.

Le Facteur Humain : Première Ligne de Défense

LE PROBLÈME

90% des attaques exploitent l'erreur humaine.

LA SOLUTION

Transformer la peur en réflexe.

ROI : 1 € investi = **3,80 €** économisés.

-68% de **taux d'erreur** après 12 mois de formation.

NIS2 : Obligation de formation pour **100%** du personnel.

Données SoSafe / ANSSI

Horizons 2026 : L'Automatisation de la Menace

IA vs IA

Agents autonomes offensifs vs Défense automatisée.

Post-VPN

Transition vers l'architecture Zero Trust.
Le VPN est obsolète.

Régulation IoT

Cyber Resilience Act (Sept 2026).
Responsabilité des fabricants.

Feuille de Route Stratégique

1. ☒ **CONFORMITÉ** : Vérifier statut EE/EI et s'inscrire sur MonEspaceNIS2.
2. ☒ **AUDIT** : Cartographier la chaîne d'approvisionnement et les accès tiers.
3. ☒ **TECHNIQUE :** Durcir les équipements de bordure (Patching VPN/Firewalls) et déployer MFA.
4. ☒ **GOUVERNANCE** : Former le COMEX (Obligation légale).
5. ☒ **CULTURE** : Investir dans la simulation de phishing et la défense humaine.

“La cybersécurité n’est plus une fonction support, c’est une condition de survie.”