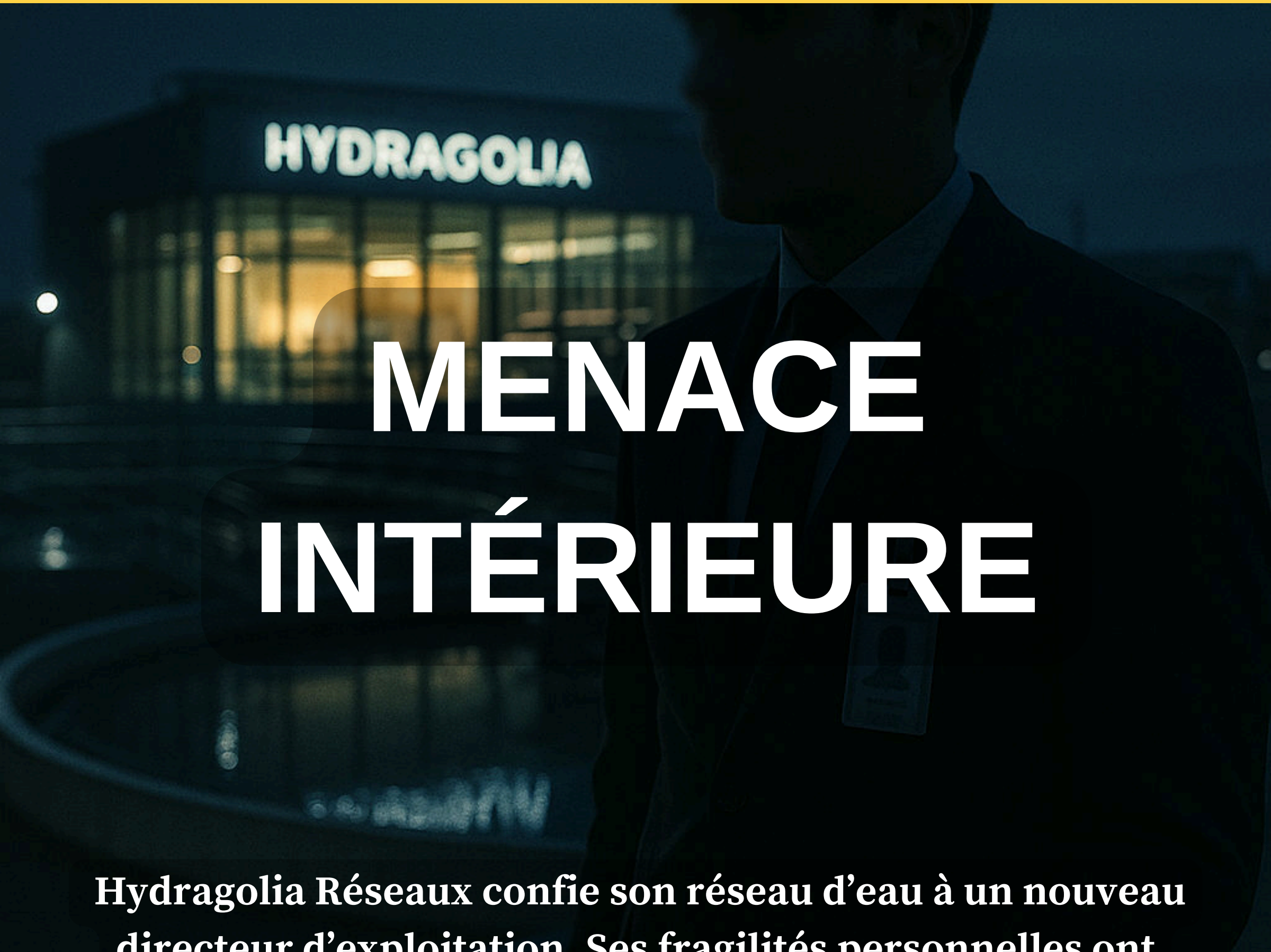
Quand le nouveau directeur devient une brèche



Hydragolia Réseaux confie son réseau d'eau à un nouveau directeur d'exploitation. Ses fragilités personnelles ont déjà été repérées par ceux qui veulent transformer un poste clé en vulnérabilité.

Le Voyage d'une menace

Épisode 10

Semkel
Renseignement & gestion des risques

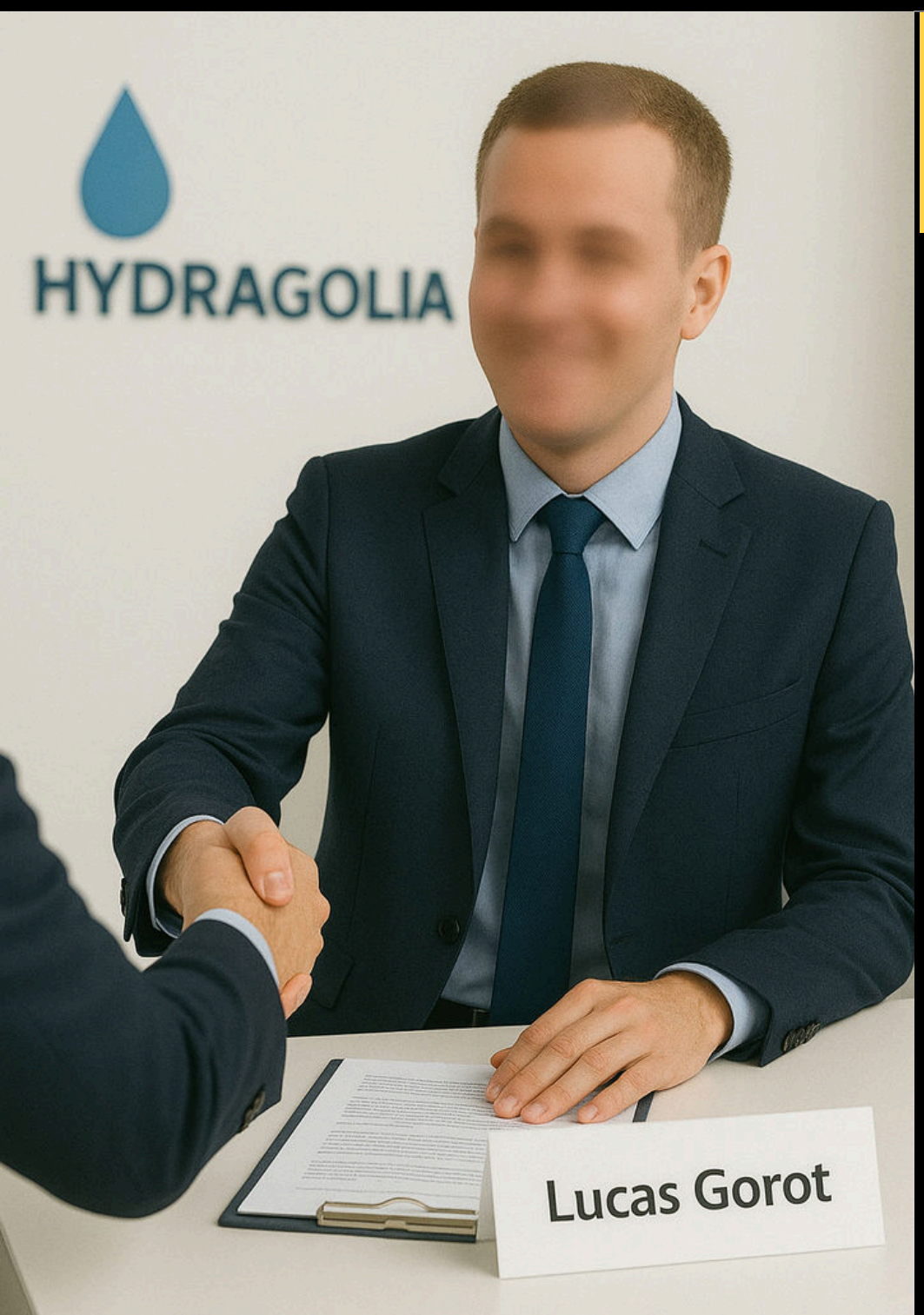
HYDRAGOLIA RÉSEAUX

HYDRAGOLIA RÉSEAUX gère l'eau potable et l'assainissement de grandes métropoles européennes :

- 20 millions d'habitants concernés.
- 7 usines de traitement, des dizaines de stations de pompage.
- Des systèmes industriels (SCADA) connectés pour optimiser la consommation, surveiller les niveaux, ajuster la qualité de l'eau.

Depuis plusieurs années, Hydragolia investit massivement dans la digitalisation. Les équipes sont fières : **"L'eau 4.0, c'est chez nous".**

Mais comme souvent, l'humain reste le point le plus fragile.



LE RECRUTEMENT

Hydragolia recrute **un nouveau directeur d'exploitation du réseau Nord** : Lucas GOROT, 42 ans, CV impeccable. 15 ans d'expérience dans l'industrie, a été entrepreneur dans l'énergie, habitué aux environnements régulés.

Le poste est critique : Lucas supervisera trois usines de traitement et plusieurs réservoirs, avec accès aux systèmes de supervision.

Le recrutement est rapide : le précédent directeur est parti brusquement, la direction veut aller vite.
On vérifie : le diplôme, deux références professionnelles… A**ucun "background check" approfondi, aucune analyse de ses fragilités ou de son environnement.**

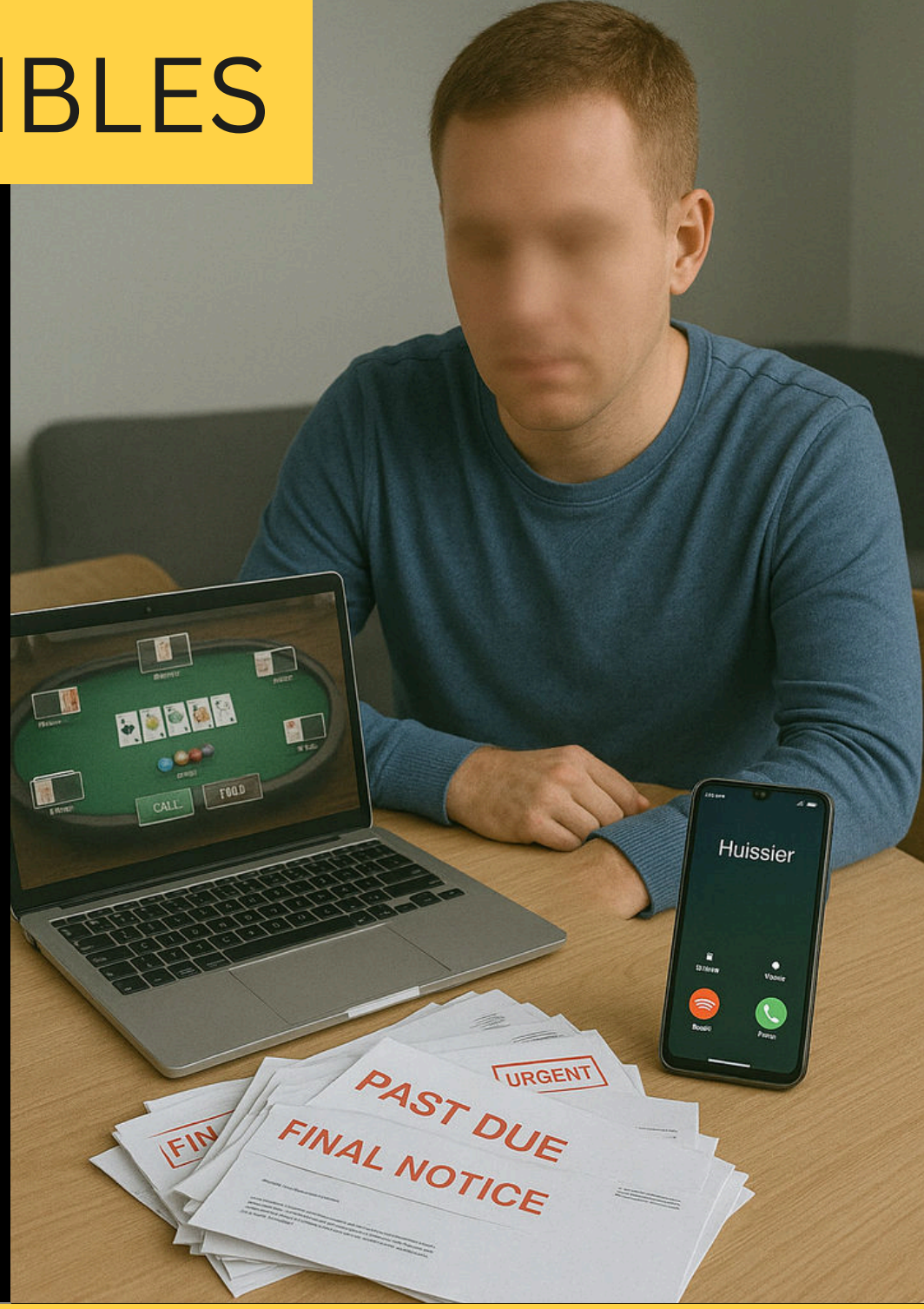
LES FRAGILITÉS INVISIBLES

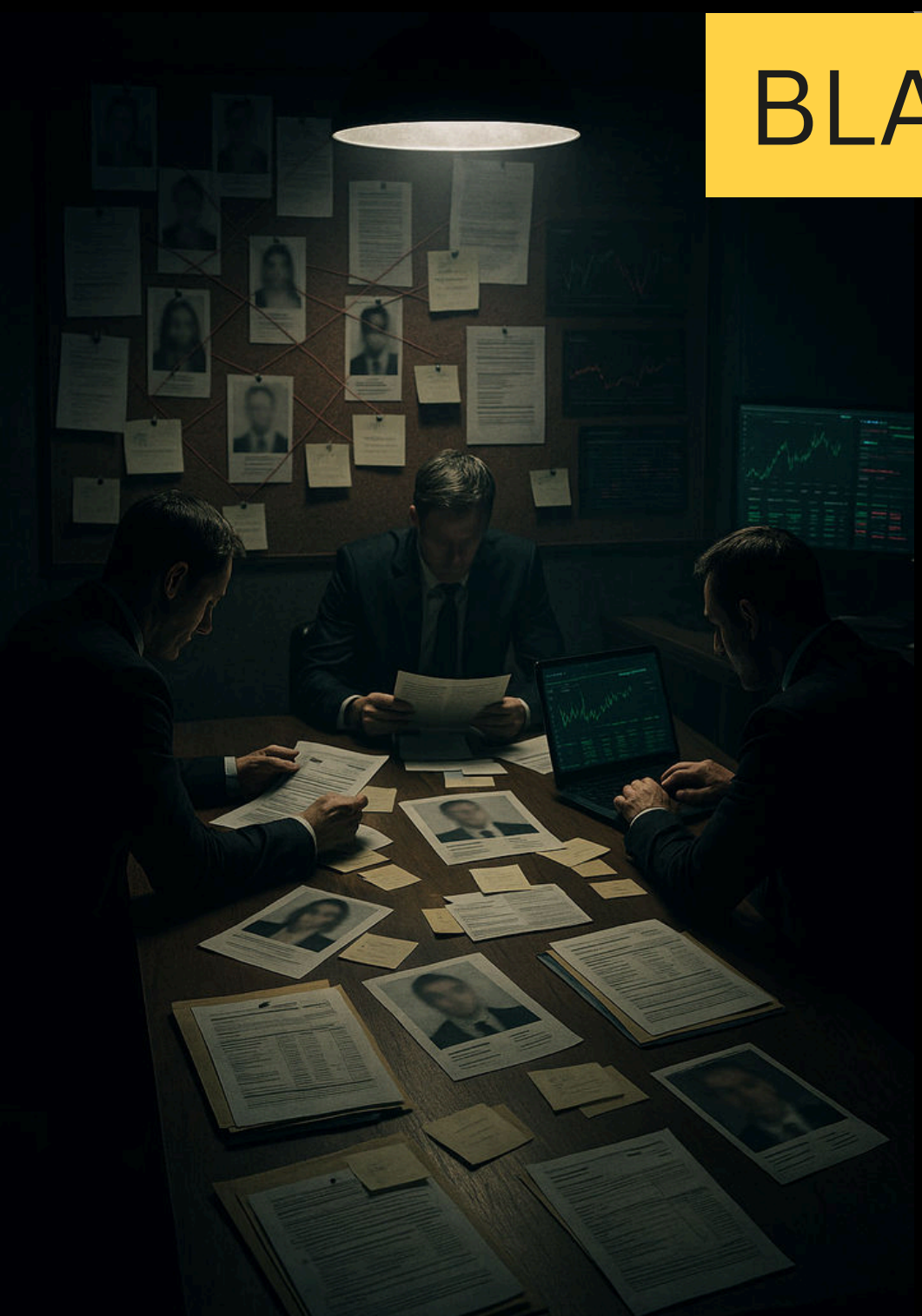
Le profil de Lucas est parfait. Sa vie personnelle, beaucoup moins : divorce avec une pension élevée à verser, joueur compulsif (poker, casino…), endetté pour compenser ses pertes.

Depuis quelques mois, il reçoit des relances d'huissiers et de sociétés de recouvrement : certaines procédures sont disponibles, notamment celle concernant son ex-entreprise qui a fait faillite il y a 3 ans.

Son nom, présent dans des parties de poker publiques, masque sa présence dans des cercles de jeu plus opaques.

Une cible idéale.





BLACK LEDGER NETWORK

Dans l'ombre, une petite cellule mêlant cybercriminels et intermédiaires douteux (BLN) scrute les fuites de données, les réseaux sociaux professionnels et les décisions de justice à la recherche de la cible idéale.

Leur objectif : repérer des profils à haut niveau sur lesquels faire pression.

Un analyste tombe sur Lucas : nouveau poste sensible, des dettes et des liens avec des réseaux clandestins de jeu.

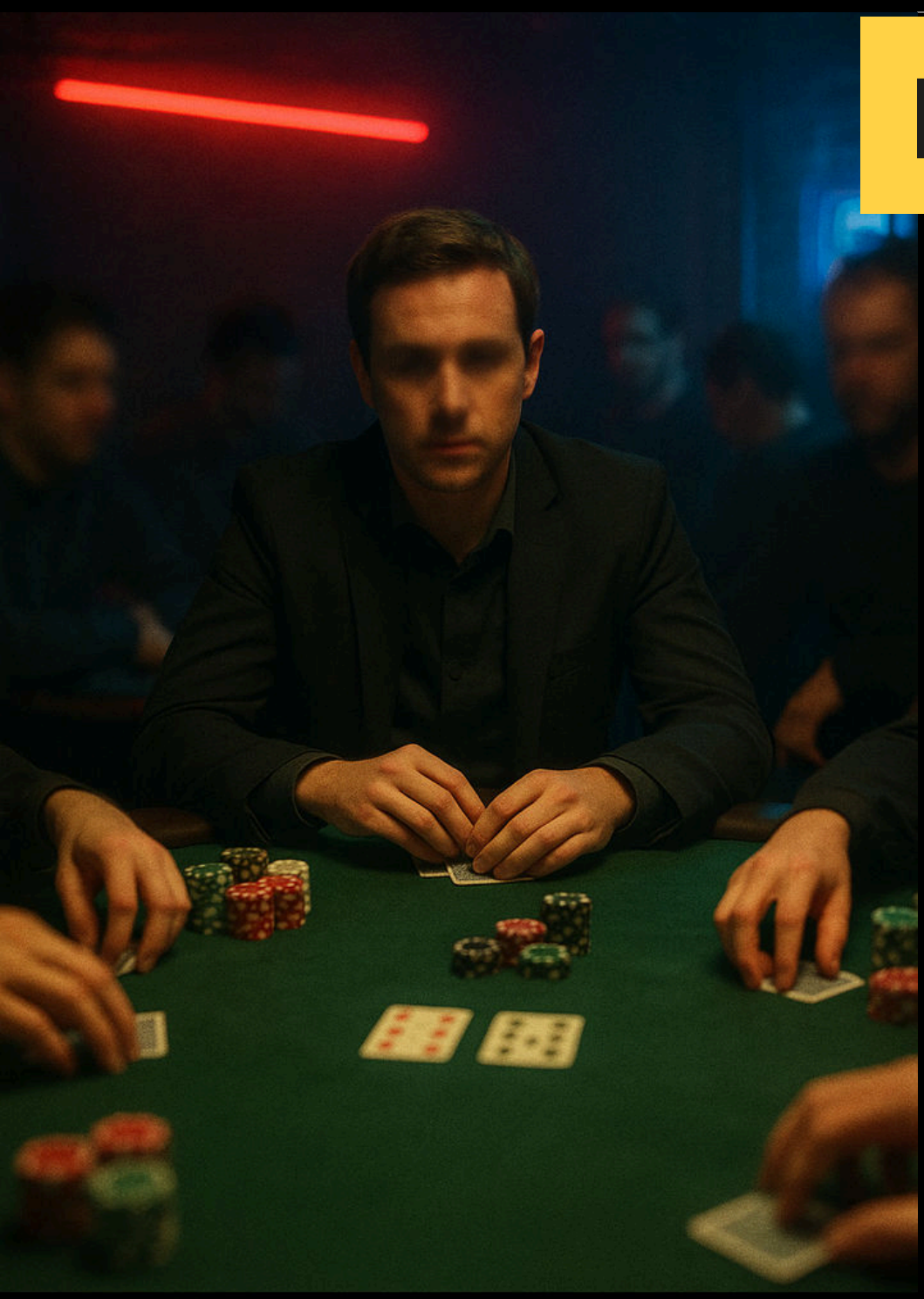
Ils décident de l'approcher pour cibler Hydragolia.

LA PROPOSITION

Lucas reçoit un jour un message d'un "conseiller financier spécialisé dans le rachat de dettes" chez HaloBank Partners, une "nouvelle startup fintech".

Le premier contact téléphonique est rassurant : on lui propose de regrouper ses crédits, de "repartir à zéro" et même la possibilité d'obtenir de l'argent supplémentaire.

Lucas saute sur l'occasion et contractualise ce nouveau prêt avec ce nouvel acteur bancaire.



MISE SOUS PRESSION

Quelques semaines plus tard, nouvel appel : "On t'a aidé, maintenant à toi de nous aider, rien de grave, juste des infos techniques."

Lucas ne comprend pas comment une banque peut lui demander ça ! **Le masque tombe et le ton devient plus menaçant :** "Lucas, nous ne sommes pas banquiers, maintenant tu nous dois de l'argent et nous savons tout de toi et même quels cercles clandestins tu fréquentes."

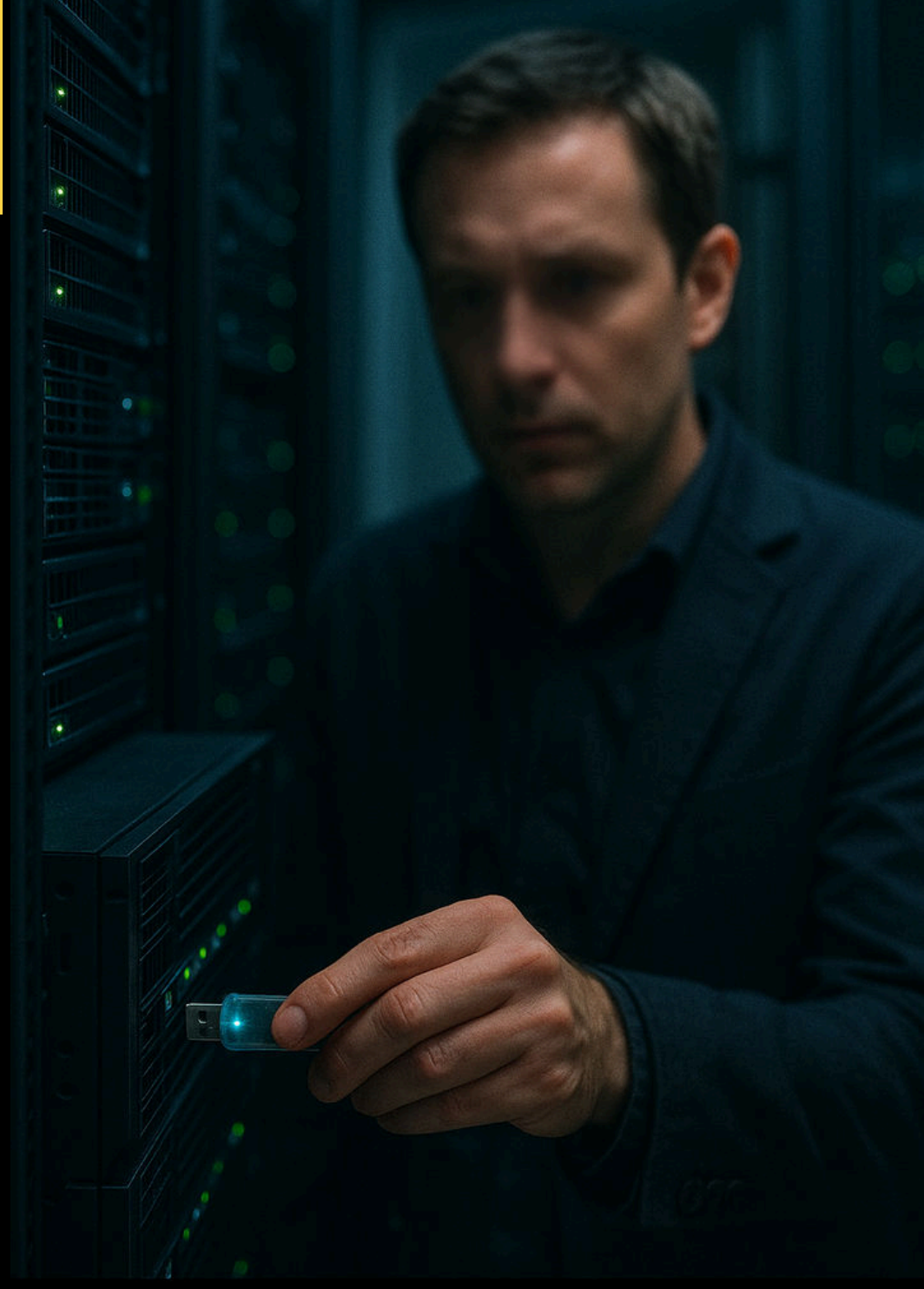
Pour preuve, il lui envoie une photo de sa dernière partie de poker avec comme menace de la donner à son ex-femme. **Il pourrait perdre la garde alternée. Lucas cède.**

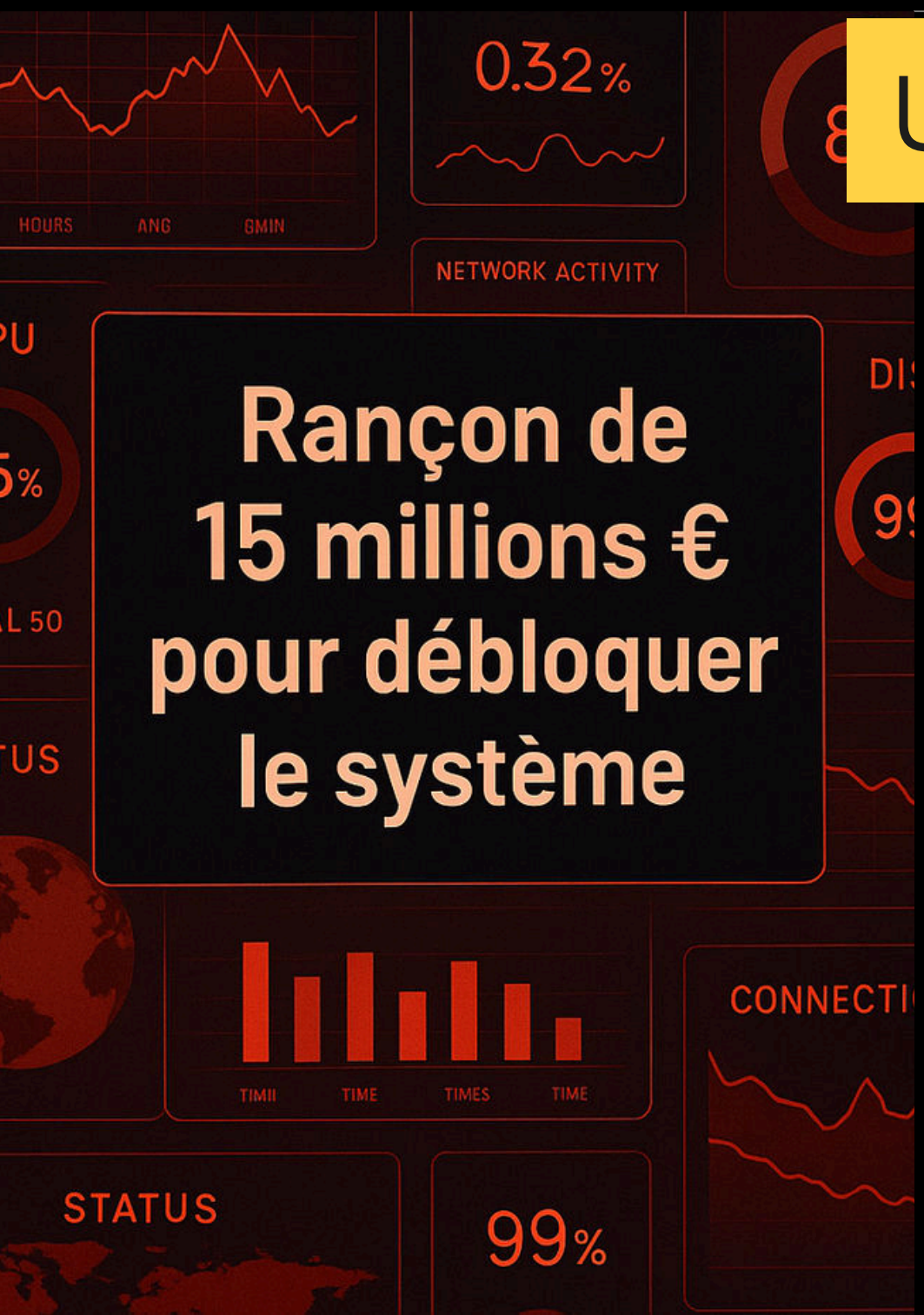
LA PRÉPARATION

D’abord, on lui demande des schémas d’architecture de son réseau et les procédures d’astreinte. Puis :

- D’ouvrir un accès VPN “temporaire” pour un prestataire supposé,
- De désactiver un contrôle d’alerte pendant un week-end de maintenance,
- De transmettre les dates des révisions majeures.

Lucas s’exécute, sans mesurer les conséquences. Il vient de devenir un maillon d’une attaque de grande ampleur.





UN RÉSEAU À GENOUX

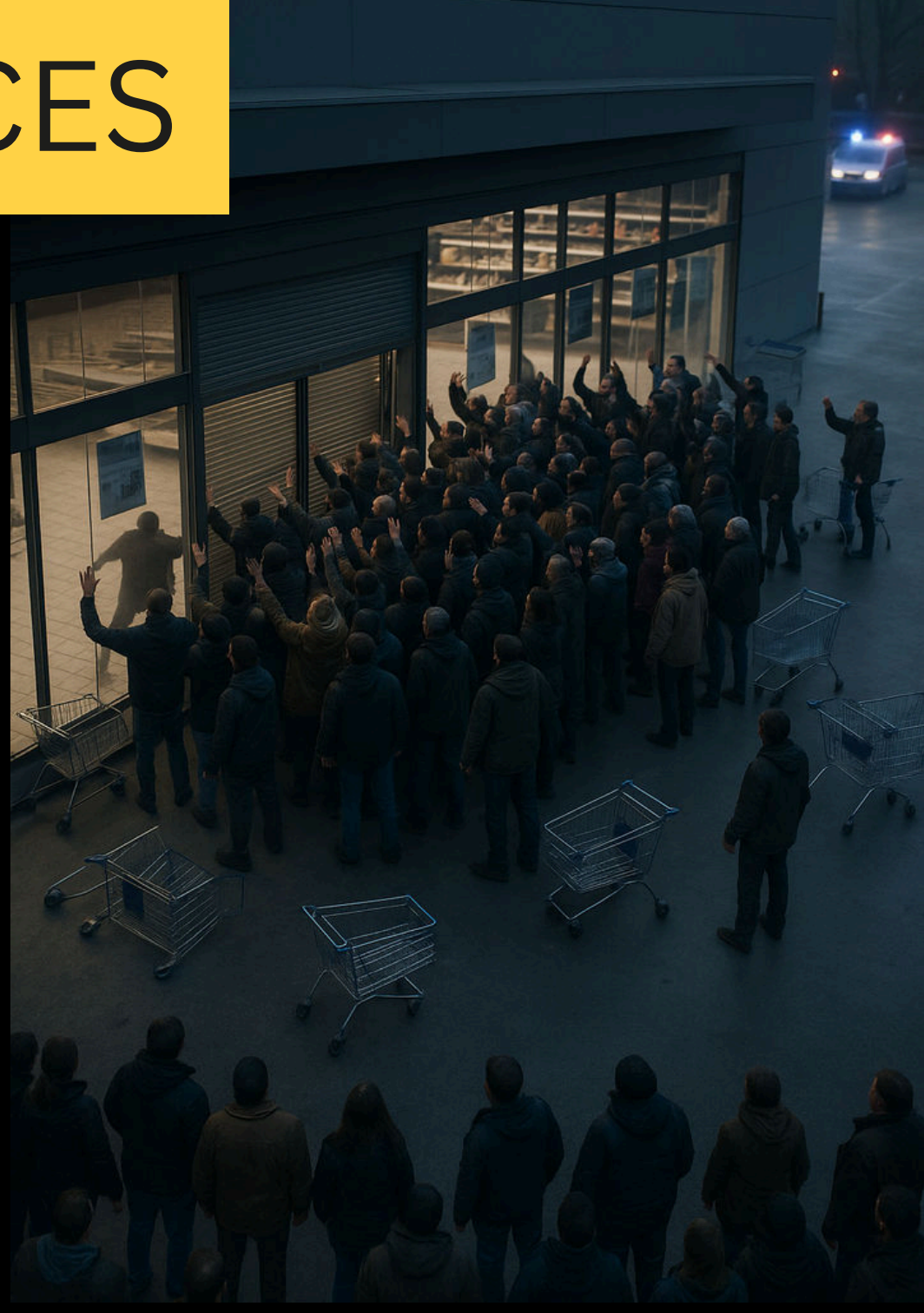
Un lundi matin, quelque chose cloche sur le réseau Nord :

- Les capteurs remontent des valeurs incohérentes.
- Des automates se mettent en sécurité.
- Une usine de traitement se coupe automatiquement pour éviter de distribuer une eau potentiellement non conforme.

Les équipes d’exploitation pensent d’abord à un bug. En réalité, les attaquants utilisent les accès obtenus via Lucas pour perturber le fonctionnement puis bloquer tout le réseau Nord.

La somme de 15 millions d’euros est demandée par BLN pour tout débloquer.

LES CONSÉQUENCES



La crise est systémique : 6 millions d'habitants sans eau potable.

Les autorités dépêchent les meilleurs experts pour relancer le réseau. La pression est immense, les réseaux sociaux et les médias sont en boucle sur le sujet.

En parallèle, **des enquêteurs commencent à retracer la chronologie des faits**. L'absence du directeur d'exploitation, Lucas Gorot, pendant la gestion de crise, éveille les soupçons. En effet, face aux conséquences de ses actes, Lucas a pris peur et est introuvable.

Les experts informatiques arrivent à retracer les brèches qui ont permis le sabotage et la prise de contrôle du système. Leur conclusion reboucle les soupçons des enquêteurs : Lucas Gorot est celui qui a permis l'attaque. Lors des perquisitions dans les vingt-quatre heures suivant l'attaque : les enquêteurs retrouvent la trace des échanges entre Black Ledger Network et Lucas, ce qui permet aux experts informatiques de mieux comprendre les outils utilisés pour le chiffrement. BLN est un acteur connu des services cyber des États.

Trente-six heures après le début de la paralysie, le réseau est enfin rétabli. On a frôlé la catastrophe : des mouvements de foule pour obtenir de l'eau en bouteille commençaient déjà à laisser présager le pire. **Les cas de ransomware ne se terminent pas toujours aussi bien, la moyenne de blocage est généralement de deux mois.**

COMMENT ÉVITER LE RISQUE INTERNE ?

Hydragolia ne pouvait pas tout anticiper. BLN aurait certainement attaqué d'une manière ou d'une autre le réseau. Néanmoins, le manque de procédures a facilité la vie des cybercriminels.

Voici quelques recommandations :

1 Faire des vérifications d'antécédents (background-check) sur les postes critiques

Une analyse d'honorabilité et de moralité est nécessaire pour les postes clés. La vérification des antécédents et de la réputation peut se faire dans le respect du cadre légal en prévenant les candidats. Les entreprises peuvent ainsi réduire le risque de menaces internes comme les conflits d'intérêts, les vulnérabilités, etc....

2 Cartographie des risques internes et procédures

Une cartographie des systèmes critiques et des risques internes attachés sont obligatoires pour pouvoir établir un plan de continuité d'activités. La mise en place de procédures de "double regard" pour les modifications critiques doit faire partie des procédures de base

3 Signaux faibles et gestion des risques

Enfin, toutes les entreprises doivent mettre en place une surveillance minimale des signaux faibles, qu'ils soient internes (procédure anormale, panne à répétition...) ou externes (rencontres fortuites, données exposées sur le dark web...). Cette gestion des risques proactive permet d'anticiper les menaces et d'en atténuer les effets.

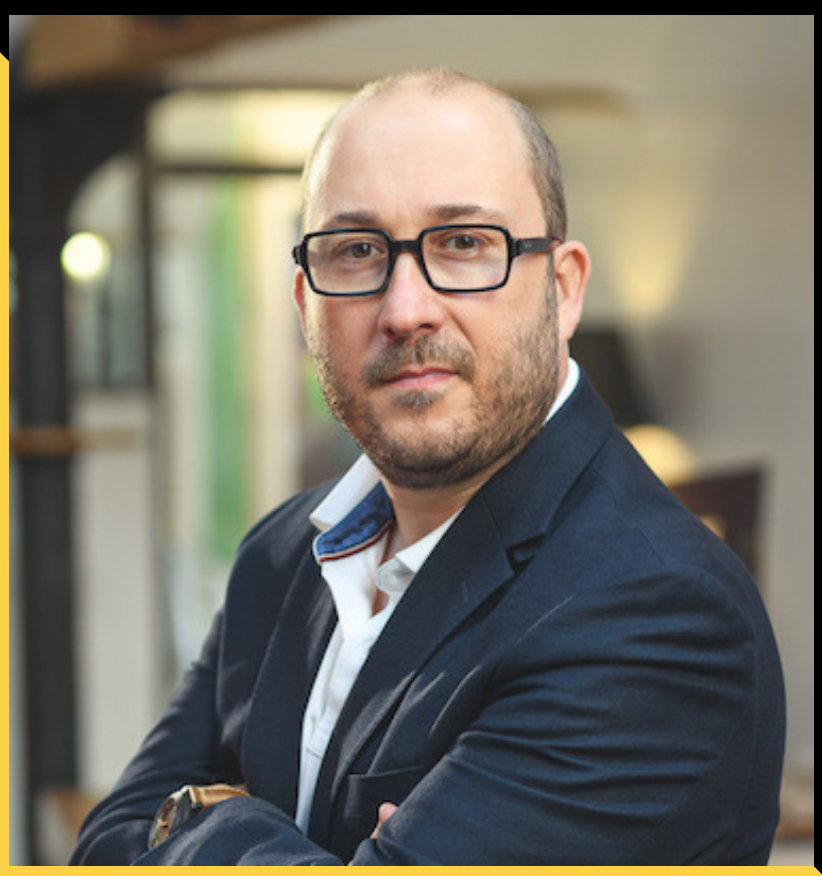
Semkel

Renseignement & gestion des risques

Avec SEMKEL, soyez résilients, préparés et accompagnés en cas de crise :

Renseignement sur la menace - Investigation OSINT - Investigation d’honorabilité et de réputation - Gestion des risques (cartographie, surveillance 24/7)

Experts en renseignement et en gestion des risques, nous proposons un accompagnement complet jusqu’à l’influence et la gestion de crise grâce à notre partenariat avec le cabinet 2017.



“ NE SUBISSEZ PLUS, ANTICIPEZ ”

Julien Lopizzo PDG de Semkel

Informations sur
contact@semkel.com ou
au +33 (0) 4 78 51 13 79