

Le Manuel de l'Enquêteur Numérique

Guide de criminalistique pour l'ingénieur réseau

DÉFINITION

La criminalistique numérique est l'enquête sur cybercrimes dans le but de recueillir des preuves d'étayer une hypothèse, de sécuriser un système ou de poursuivre un criminel.

LES 5 OBJECTIFS TACTIQUES

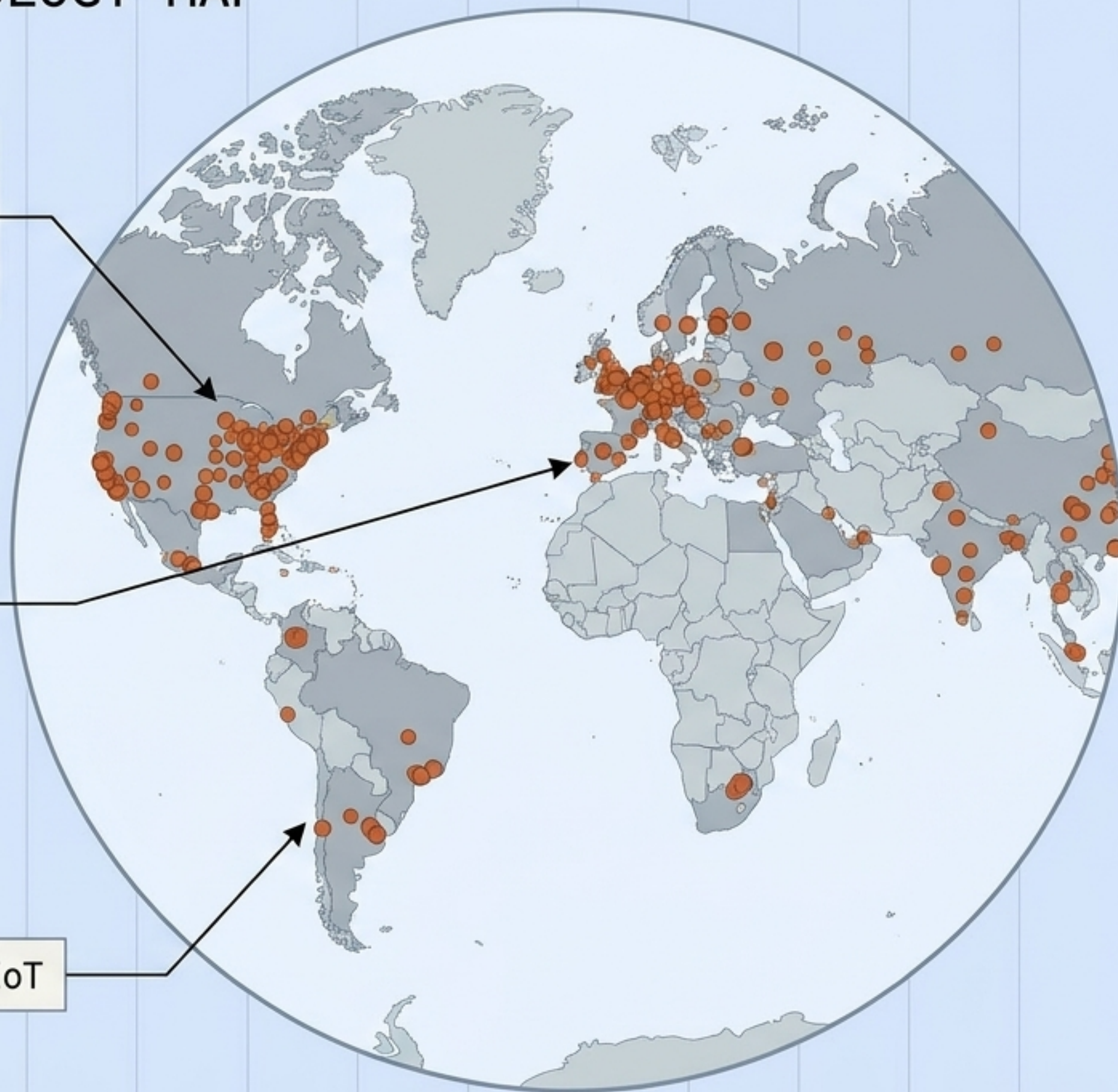
1.  Recueillir des preuves utiles (Traçabilité).
2.  Ne pas interrompre les processus opérationnels.
3.  Garantir un impact positif sur les actions en justice.
4.  Persuader les adversaires de renoncer aux attaques.
5.  Maintenir un coût de procédure acceptable.

THREAT TOPOLOGY MAP

SYSTÈMES DE
CONTRÔLE
INDUSTRIELS
(SCADA) EXPOSÉS

SERVEURS FTP
NON SÉCURISÉS

VULNÉRABILITÉS IoT

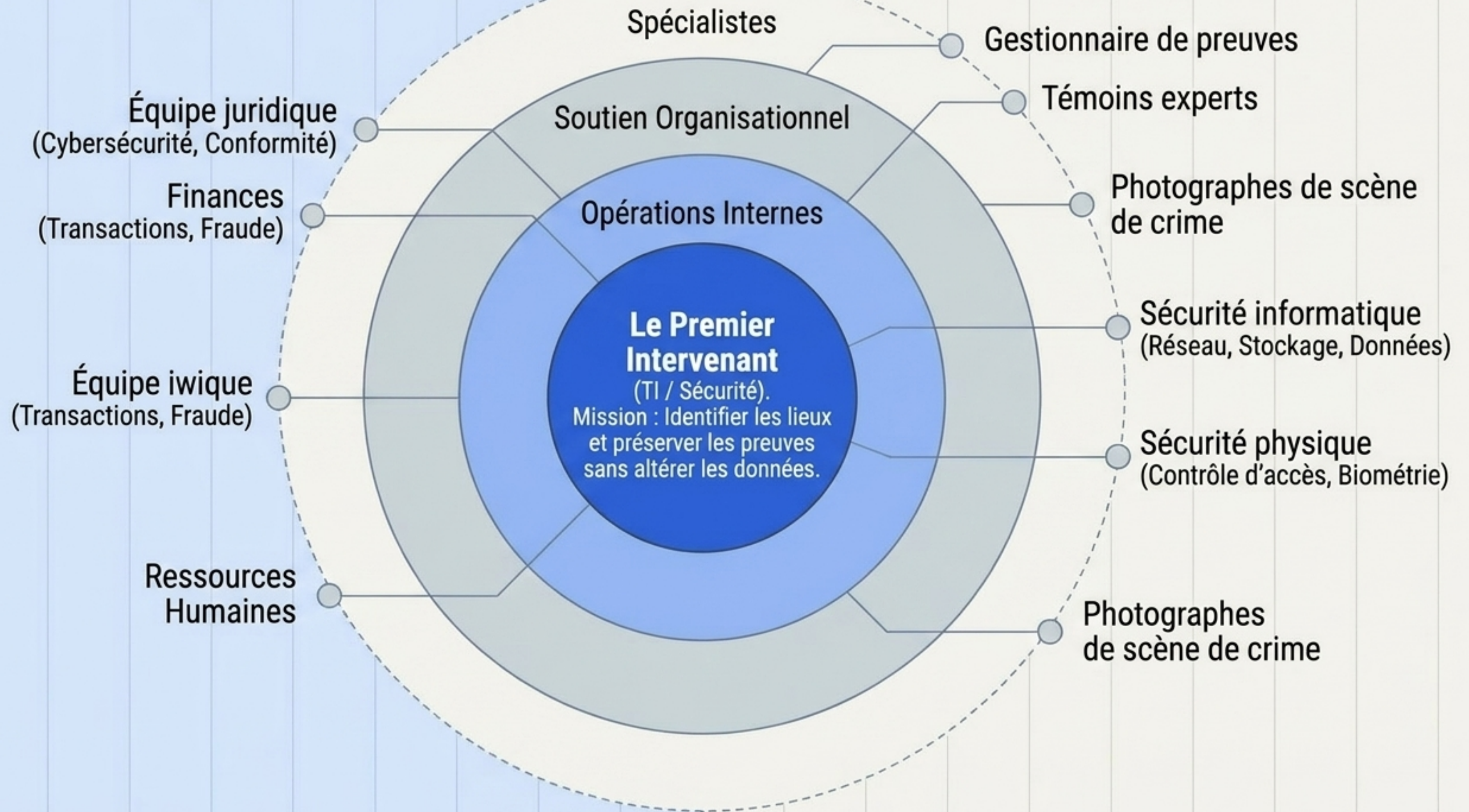


L'Internet de Tout (IdT)
élargit massivement la
surface d'attaque.

Des systèmes critiques
(comme les réseaux
SCADA) sont souvent
exposés par erreur.

La technologie et la
criminalité progressent
beaucoup plus vite que le
droit.

La capacité à mener une
enquête numérique est
devenue une compétence de
survie organisationnelle.

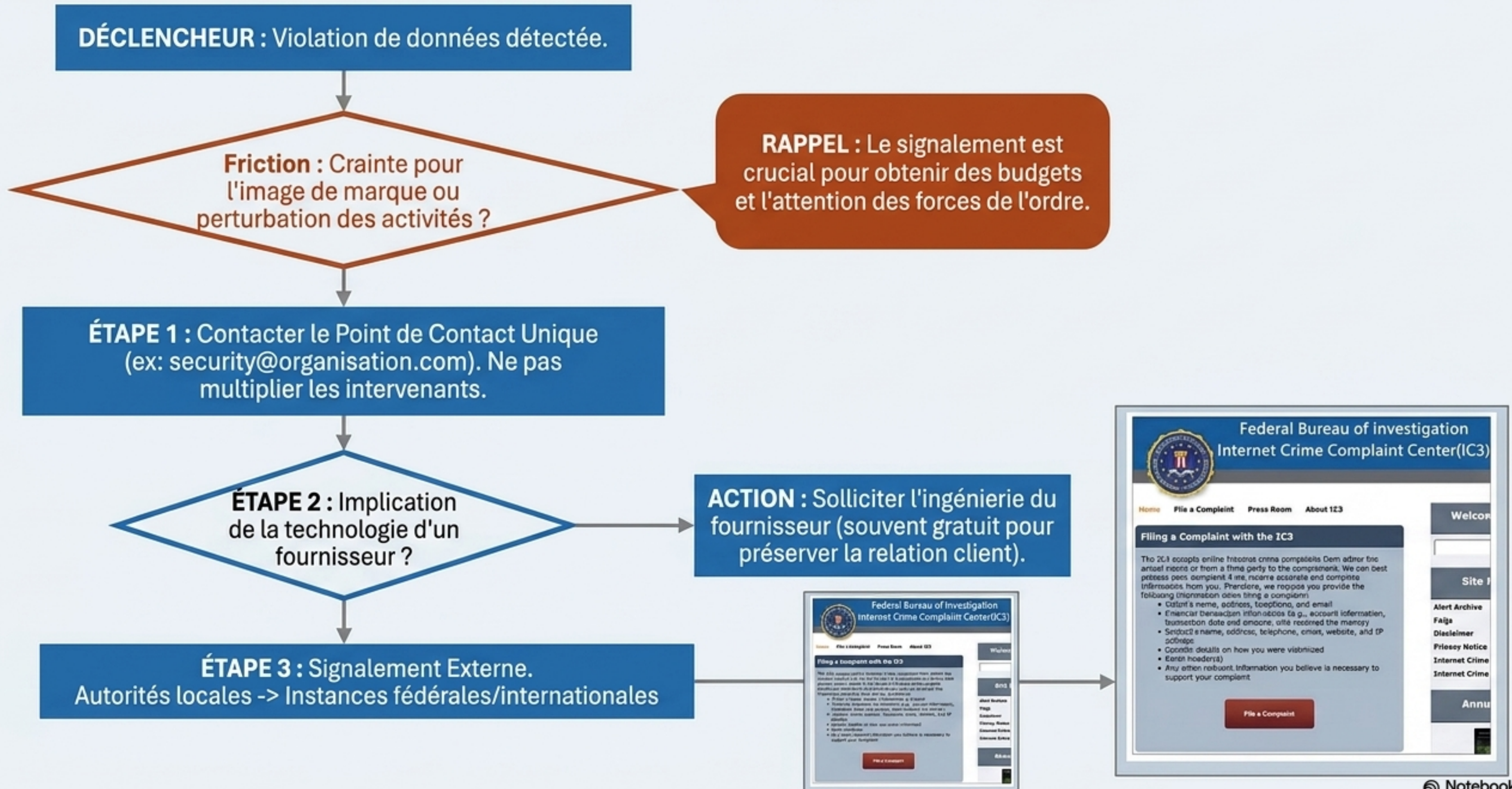


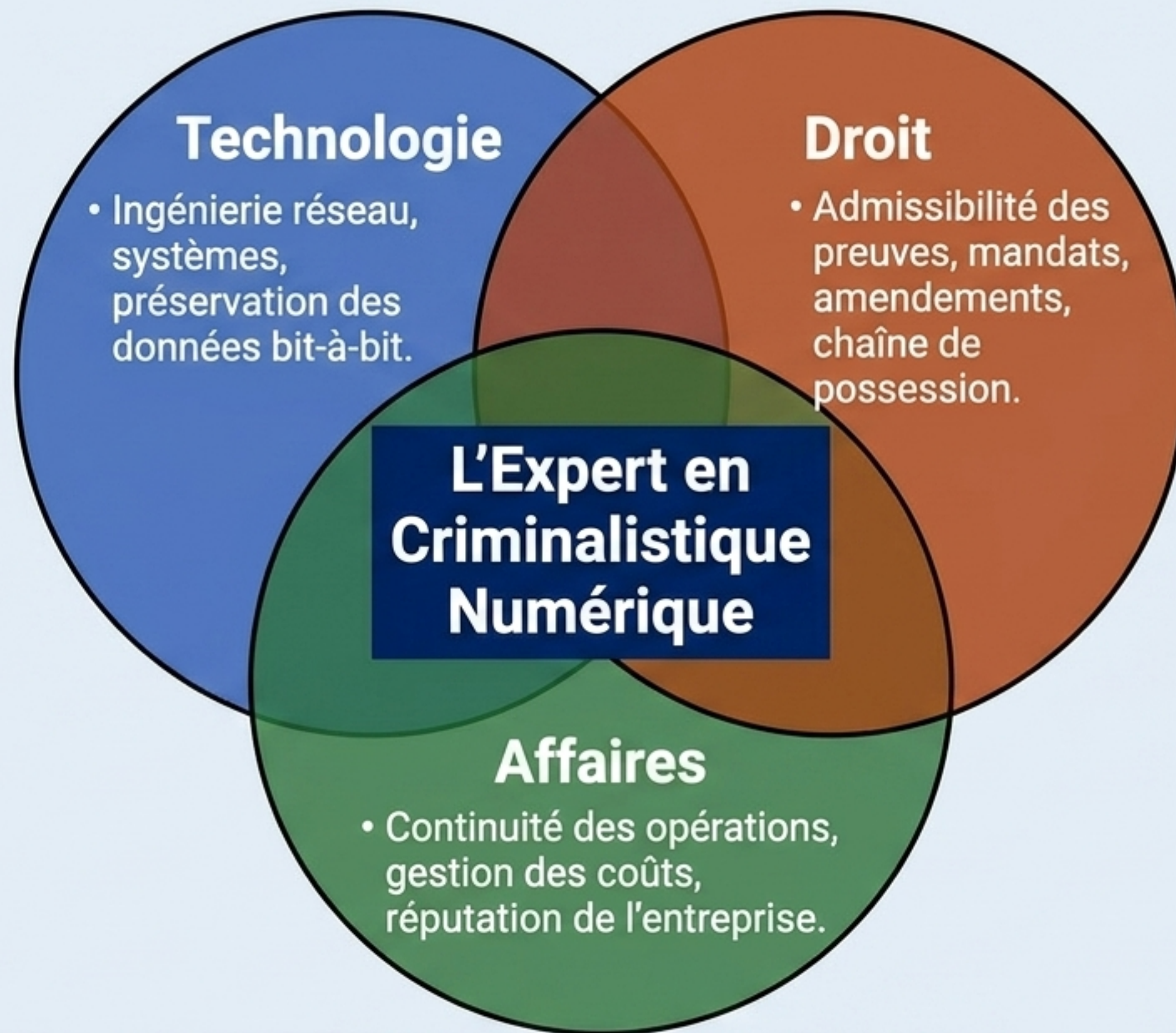
Le Dilemme : Interne vs Externe

	Services Internes	Services Professionnels Externes
Coût	Économique, développe les compétences 	Peut coûter des centaines de milliers de dollars 
Conflit d'intérêts	Risque élevé de partialité 	Garantit l'objectivité requise par les tribunaux 
Compétences & Risques	Risque de corruption des preuves si inexpérimenté	Expertise technique pointue requise pour les enjeux majeurs
Réputation	Discrétion totale	Poids juridique d'un cabinet réputé

STRATÉGIE HYBRIDE RECOMMANDÉE : Utiliser les ressources internes pour la documentation et la gestion de projet, et des spécialistes externes pour l'analyse technique critique.

Signaler ou Contenir ?





Un ingénieur réseau se concentre uniquement sur la technologie. Un expert forensique doit opérer parfaitement à l'intersection de ces trois mondes pour produire des preuves admissibles en cour sans détruire la viabilité de l'entreprise.

La Frontière Juridictionnelle : Quand la loi traîne derrière la technologie.



Le mur d'état :

Un policier de Chicago ne peut pas arrêter un criminel en Floride en raison des restrictions de juridiction.

Le mur international :

Le FBI n'est pas autorisé à arrêter un criminel en Espagne, uniquement sur les territoires sous contrôle américain.

Le vide juridique :

Des actes évidents peuvent être impossibles à poursuivre si la législation locale n'a pas encore défini l'acte comme criminel (ex: le spam avant 2003).

Le 4e Amendement : L'ordinateur comme "Conteneur Fermé"

LE PRINCIPE :

En vertu de la loi (ex: 4e amendement américain), les supports de stockage électroniques sont légalement traités exactement comme une mallette ou une armoire à dossiers verrouillée.



L'EXCEPTION CORPORATIVE :

Cette protection constitutionnelle ne s'applique pas aux perquisitions effectuées par des organismes privés (votre employeur).

RÈGLE OPÉRATIONNELLE :

Le bureau et l'ordinateur d'un employé sont considérés comme sa résidence privée SAUF si un accord de consentement explicite a été signé. Saisir un PC sans consentement détruit la preuve.

Matrice des Types de Consentement Légal

DÉFINITION	CONTEXTE	IMPLICATION TECHNIQUE
  1 Consentement Général	Accord direct du propriétaire ou d'un tiers autorisé (conjoint, admin système).	La personne doit être lucide (non ébriquée/malade) et comprendre exactement à quels droits elle renonce.
  2 Consentement Implicite	Bannières d'information informatique, cases à cocher de connexion, emballages logiciels.	Toujours exiger une signature de consentement pour tout appareil (y compris mobile) fourni par l'employeur. Crucial pour les politiques TI.

Exceptions au Mandat et Pièges Opérationnels



Preuves en évidence (Plain View) :

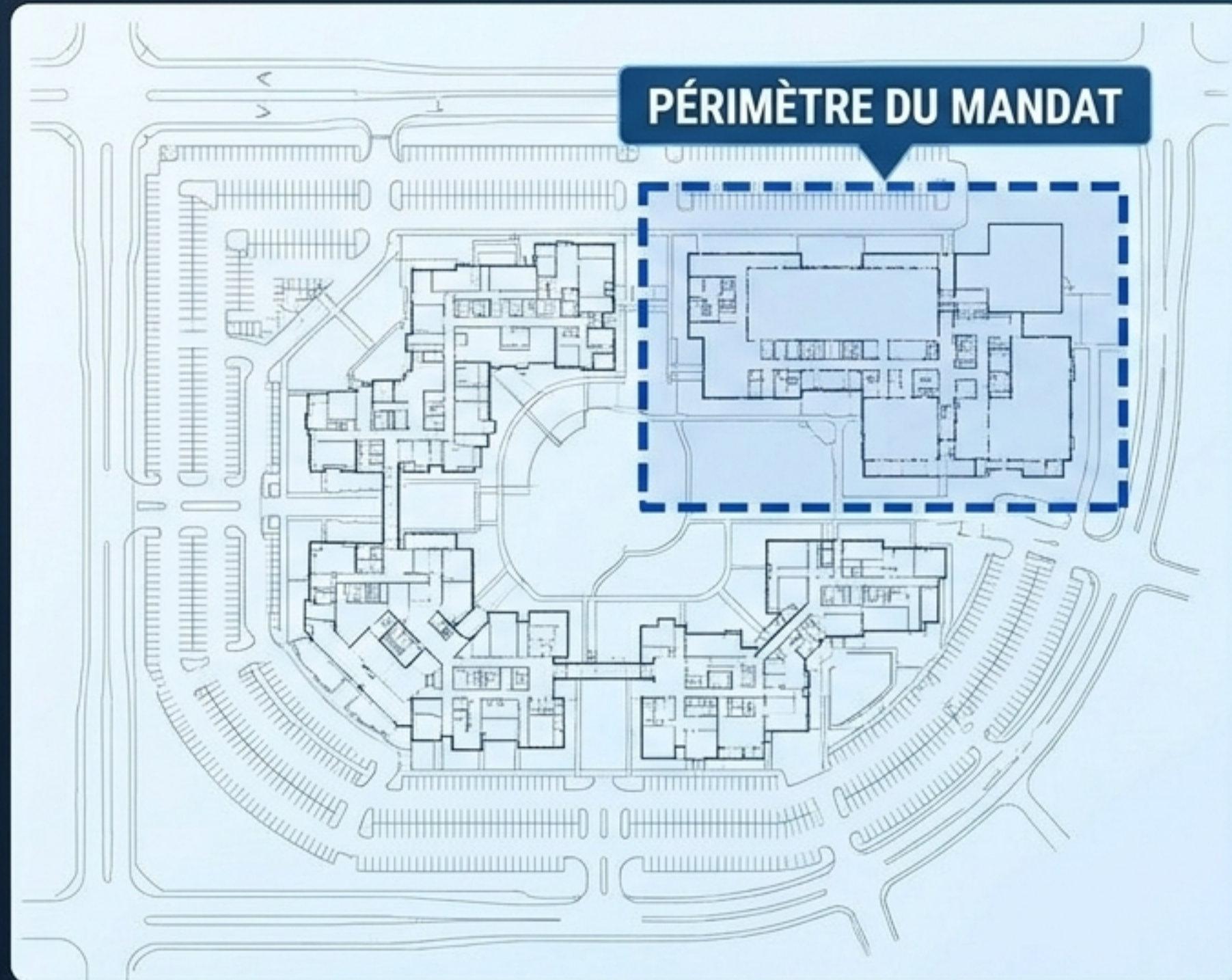
Si un fichier est déjà ouvert à l'écran, il peut être photographié sans mandat. L'agent ne peut pas ouvrir de nouveaux dossiers.

Fouille & Urgence :

Autorisé sous un simple "soupçon raisonnable" aux frontières, ou s'il y a un risque imminent de destruction des données périssables.

LE PRÉCÉDENT TOUCH-ID : Les forces de l'ordre peuvent physiquement forcer un suspect menotté à utiliser son empreinte digitale pour déverrouiller un appareil.
CONSEIL PRAGMATIQUE : Limitez les tentatives biométriques ou utilisez un code PIN pour forcer le verrouillage de l'appareil.

L'Exécution du Mandat : Portée et Limites



La Portée Physique : Les mandats limitent la zone de perquisition. Les grands campus (comme Cisco) nécessitent souvent plusieurs mandats distincts pour différents bâtiments.



Découvertes Fortuites : Si des preuves de crimes graves (ex: pornographie infantile) sont découvertes par accident lors d'une saisie réseau légale pour un autre motif, elles sont saisissables.



Mines Terrestres Juridiques

- **PPA :** [REDACTED] Protège les documents de travail et la liberté de la presse.
- **ECPA :** [REDACTED] Saisir un FAI sans protéger les données des autres clients tiers est une violation flagrante.
- **HIPAA :** [REDACTED] Exige des autorisations spéciales pour les données médicales.

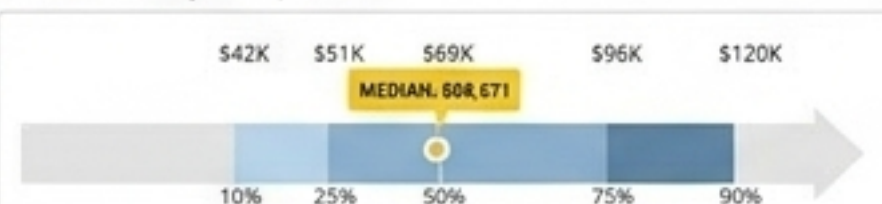
Le Marché du Travail : Une Demande en Pleine Expansion

CONCURRENCE : FAIBLE // DEMANDE : MASSIVE

SALAIRE DE DÉPART : ~90 000 \$ USD / an

Forensic Computer Analyst Salary (United States)

A Forensic Computer Analyst earns an average salary of \$68,871 per year. A skill in Computer Security is associated with high pay for this job. People in this job generally don't have more than 20 years' experience.



Add this chart to your site: [640px](#) [200px](#)

[experience](#) [skill](#) [job](#)

Show Hourly Rate

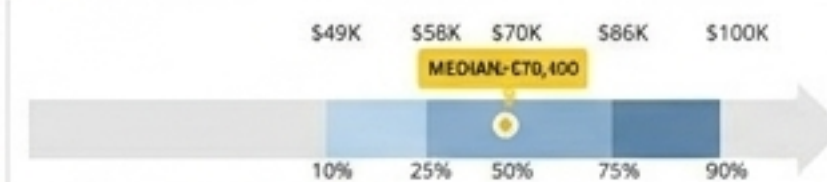
	National Salary Data (7)	\$0	\$50K	\$100K	\$150K
Salary	\$41,710 - \$117,394				
Bonus	\$1,500 - \$25,000				
Total Pay (7)	\$40,967 - \$120,007				

Country: United States | Currency: USD | Updated: 18 Jan 2017 | Individuals Reporting: 225

Information Security Analyst Salary (United States)

Earnings for Information Security Analysts in the United States come in at around \$70K annually on average. In the world of information Security Analysts, total cash

[Read More](#)



Add this chart to your site: [610px](#) [300px](#)

[city](#) [experience](#) [skill](#) [employer](#) [job](#)

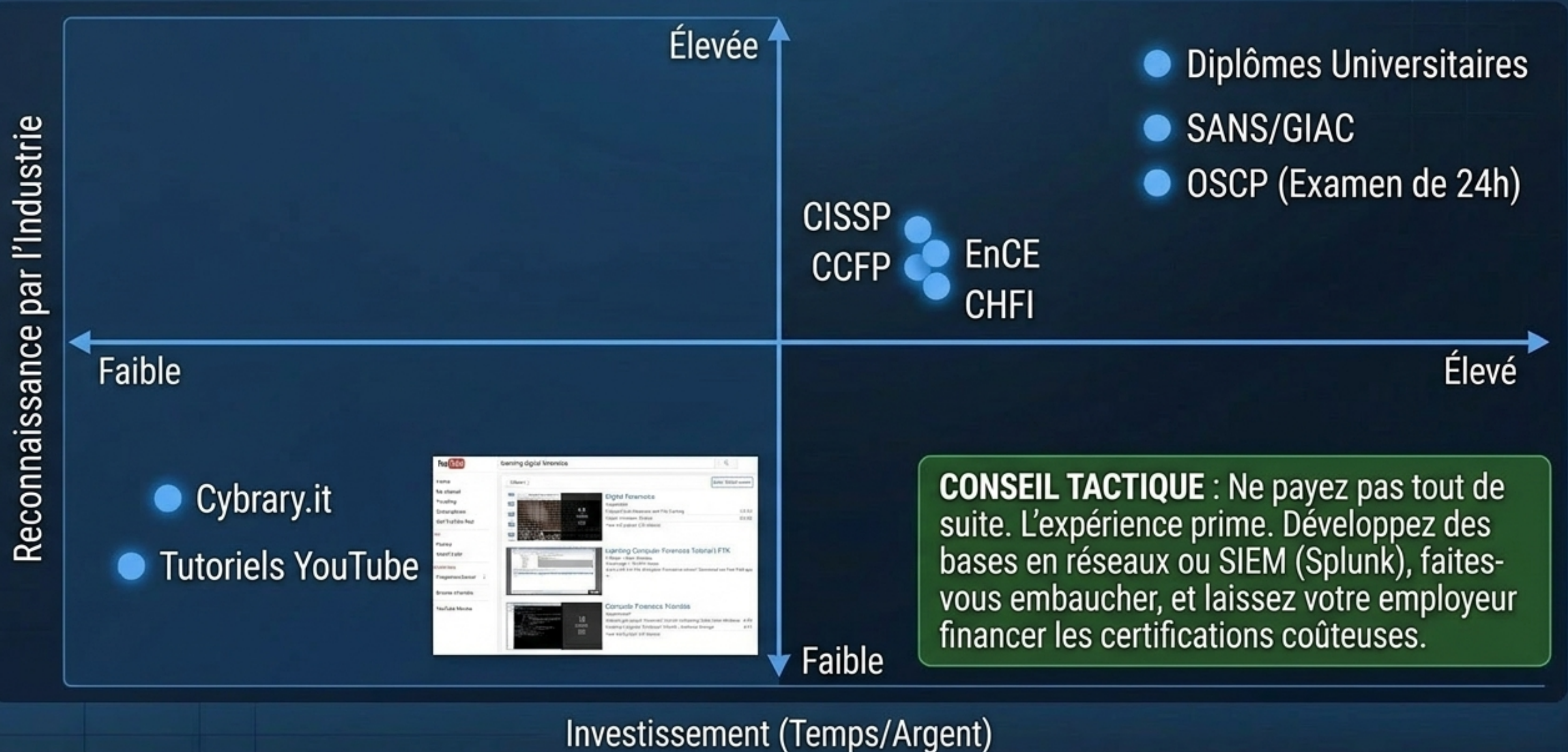
Show Hourly Rate

	National Salary Data (7)	\$0	\$50K	\$100K	\$150K
Salary	\$49,478 - \$102,185				
Bonus	\$201.80 - \$10,063				
Profit Sharing	\$0.00 - \$9,115				
Total Pay (7)	\$47,555 - \$104,537				

Country: United States | Currency: USD | Updated: 18 Jan 2017 | Individuals Reporting: 2,773

LA STRATÉGIE D'ENTRÉE : Trouver un poste spécifiquement intitulé 'Analyste Forensique' est rare pour un premier emploi. La voie stratégique consiste à exceller en cybersécurité générale ou en ingénierie réseau, puis à intégrer ces compétences d'investigation pour accéder aux postes les plus lucratifs.

Matrice d'Investissement en Formation



Le Circuit : Réseautage et Immersion

Les Géants (RSA, Black Hat)

Budget élevé, parrainages massifs, soirées onéreuses. Excellent pour la visibilité mondiale.

L'Underground Tactique (DEF CON, BSides)

BSides est gratuit. DEF CON coûte quelques centaines de dollars. Offre le même contenu technique que les grandes conférences.

Astuces de Pro pour Ingénieurs

Le prix n'est pas un gage de qualité. Négociez toujours vos formations (refusez l'iPad inclus pour baisser le prix, demandez la gratuité de l'hôtel).

La communauté de la cybersécurité est ouverte. Participez, formez-vous, et devenez la ressource rare qui maîtrise la technologie, la loi et les affaires.