

Réagir à une violation de données

Le manuel tactique et stratégique de réponse aux incidents.

« Ne confondez jamais un revers isolé avec une défaite définitive. »

Le coût de l'impréparation

eBay (Mai 2014)

233 millions de
comptes exposés.

Échec : Trois mois
pour détecter, deux
semaines
supplémentaires
pour signaler.

Hollywood Presbyterian (2016)

Paralyse
critique.

Impact : Paiement
d'une rançon de
17 000 \$ car l'hôpital
ne pouvait plus
soigner ses patients.

Yahoo! (Fév. 2017)

Impact financier
direct.

Conséquence :
Verizon réduit son
offre d'achat de
350 millions de
dollars US.

OneLogin (Mai 2017)

Perte de
confiance.

L'efficacité même du
logiciel de sécurité
remise en question
sur la place
publique.

La négligence n'est plus seulement technique, elle engendre des conséquences financières et juridiques désastreuses.

Pourquoi les organisations échouent face aux incidents

L'illusion de la conformité



Symptôme :

Investir massivement dans HIPAA ou PCI DSS et s'arrêter là.

Diagnostic :

La conformité est basée sur des normes standardisées et parfois obsolètes, pas sur les vulnérabilités réelles. C'est le niveau minimal, pas une armure.

Le syndrome « On appelle John »



Symptôme :

Aucune équipe dédiée ; panique et appel au service informatique en espérant qu'ils gèrent tout.

Diagnostic :

Refus d'admettre la nécessité d'un plan préventif. La sécurité est perçue uniquement comme un coût à réduire.

La fausse confiance des simulations



Symptôme :

Réaliser des exercices de discussion sur table dans un cadre informel et se croire prêt.

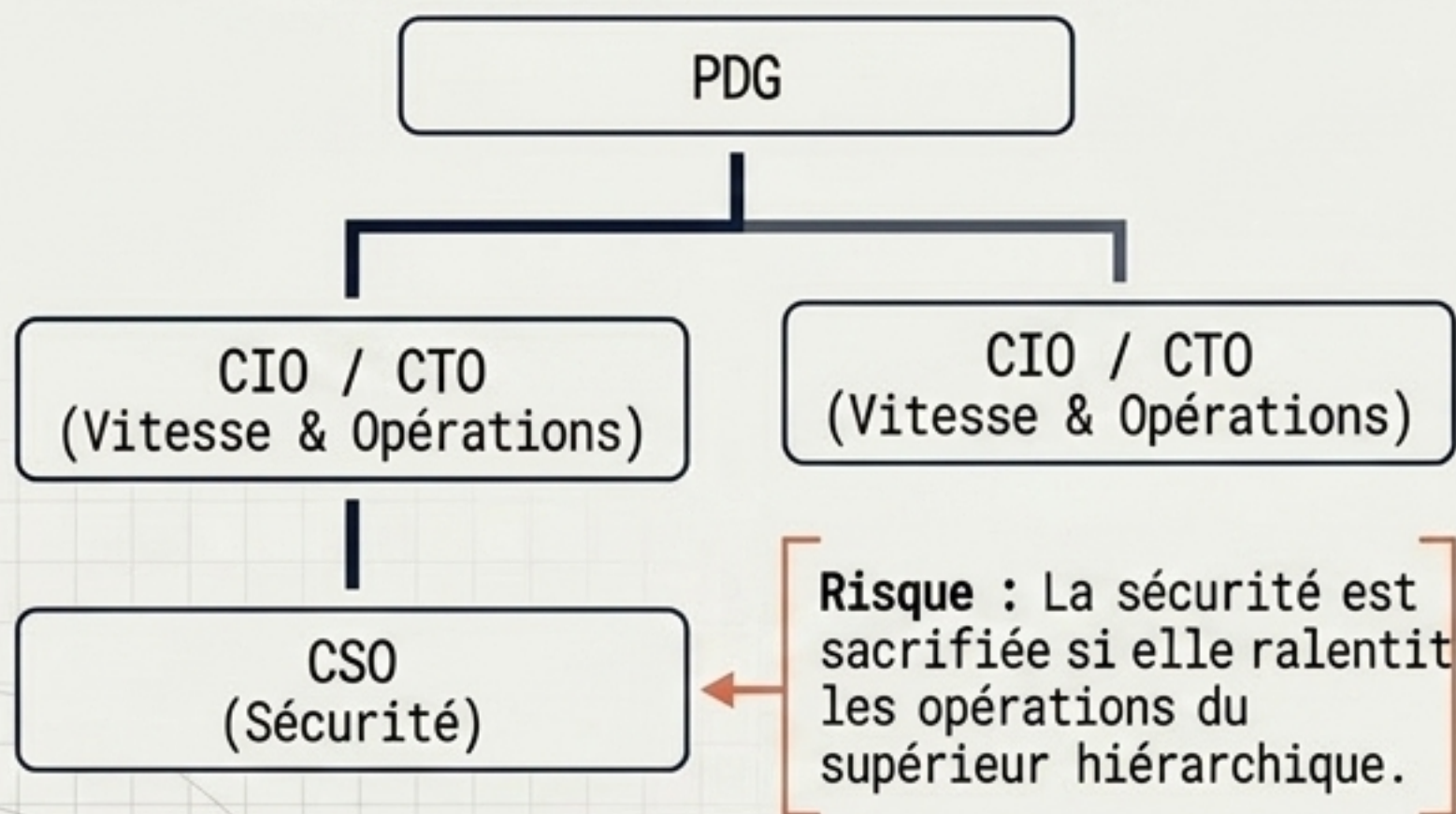
Diagnostic :

Une simulation théorique en salle de classe n'égale jamais l'intensité d'un véritable entraînement « équipe rouge vs équipe bleue » (attaque et défense).

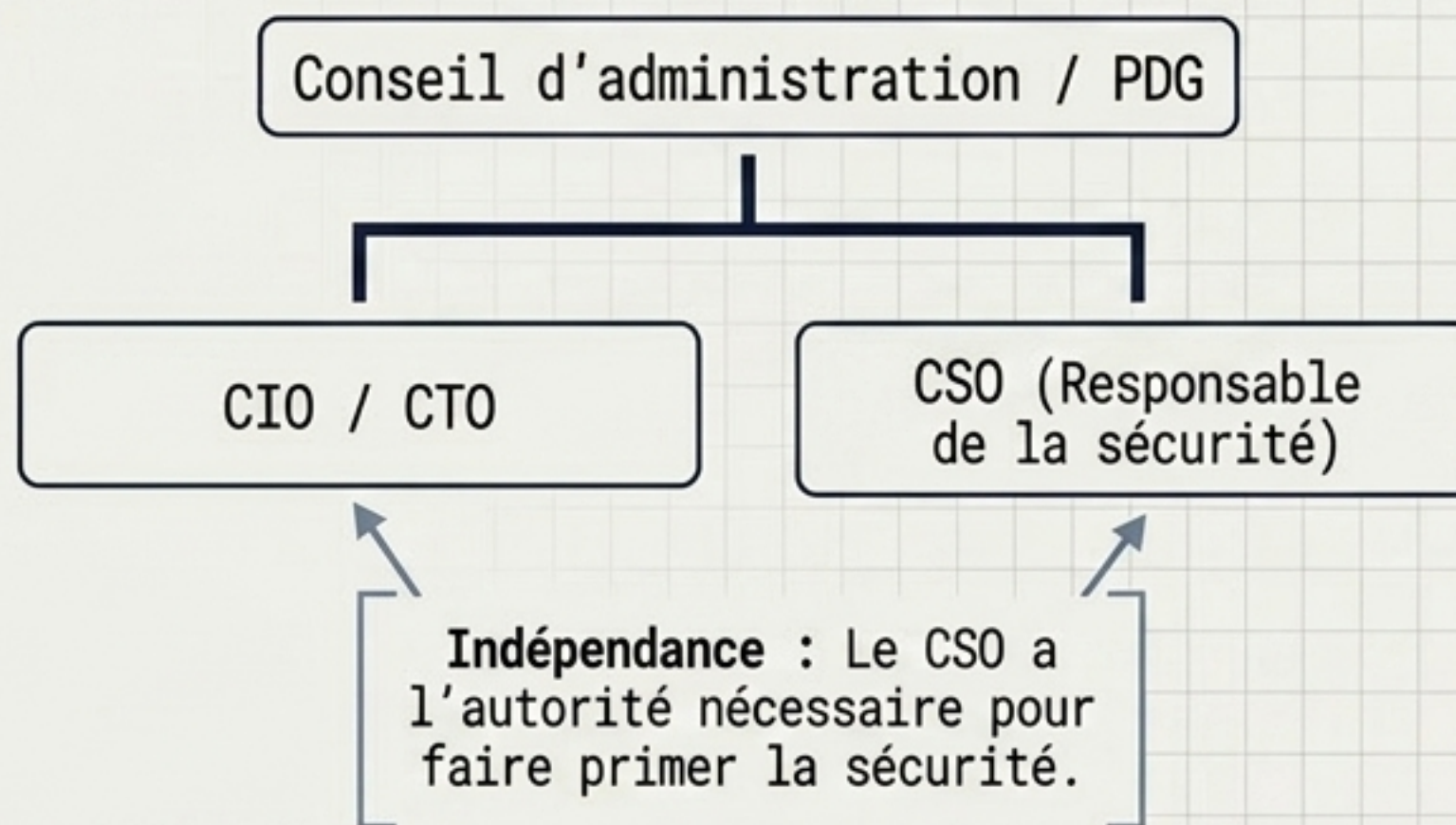
La gouvernance de la sécurité

Restructurer pour éliminer les conflits d'intérêts.

❌ Structure Défaillante

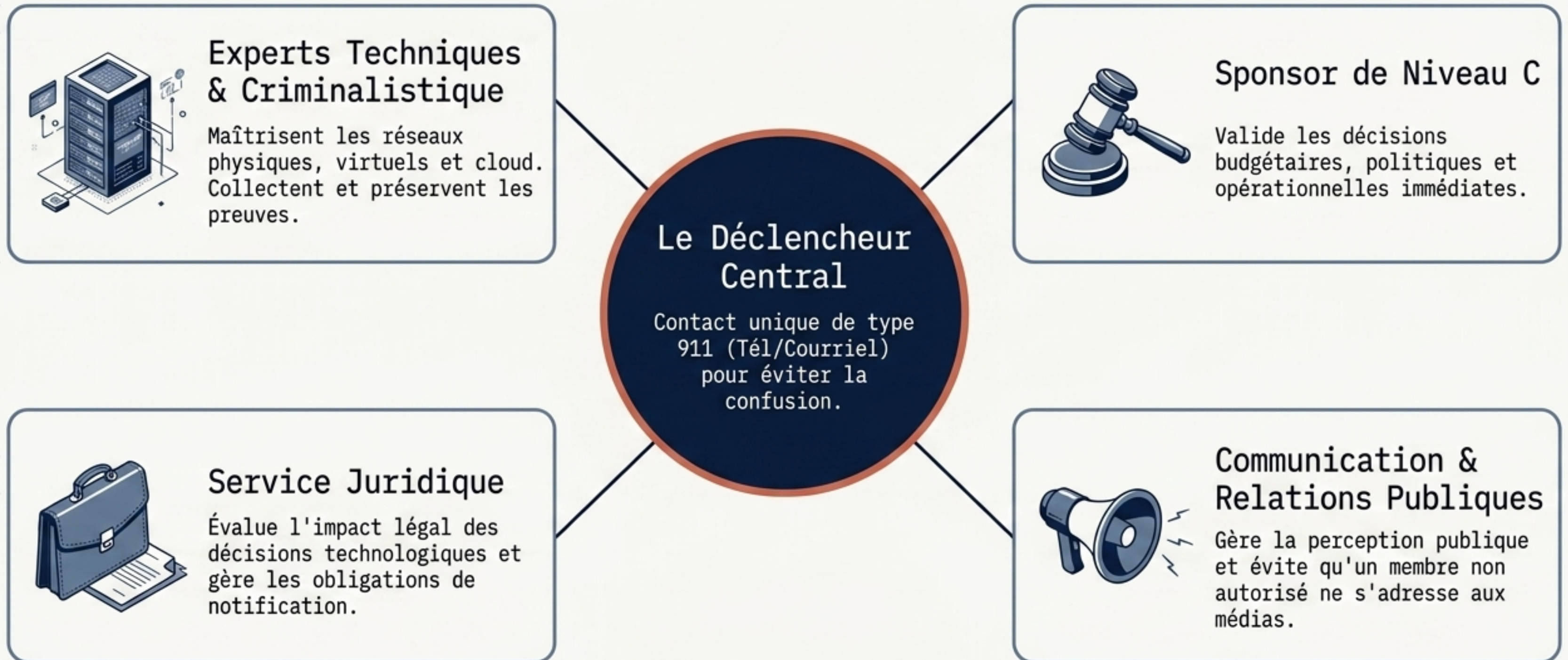


✅ Structure Optimale

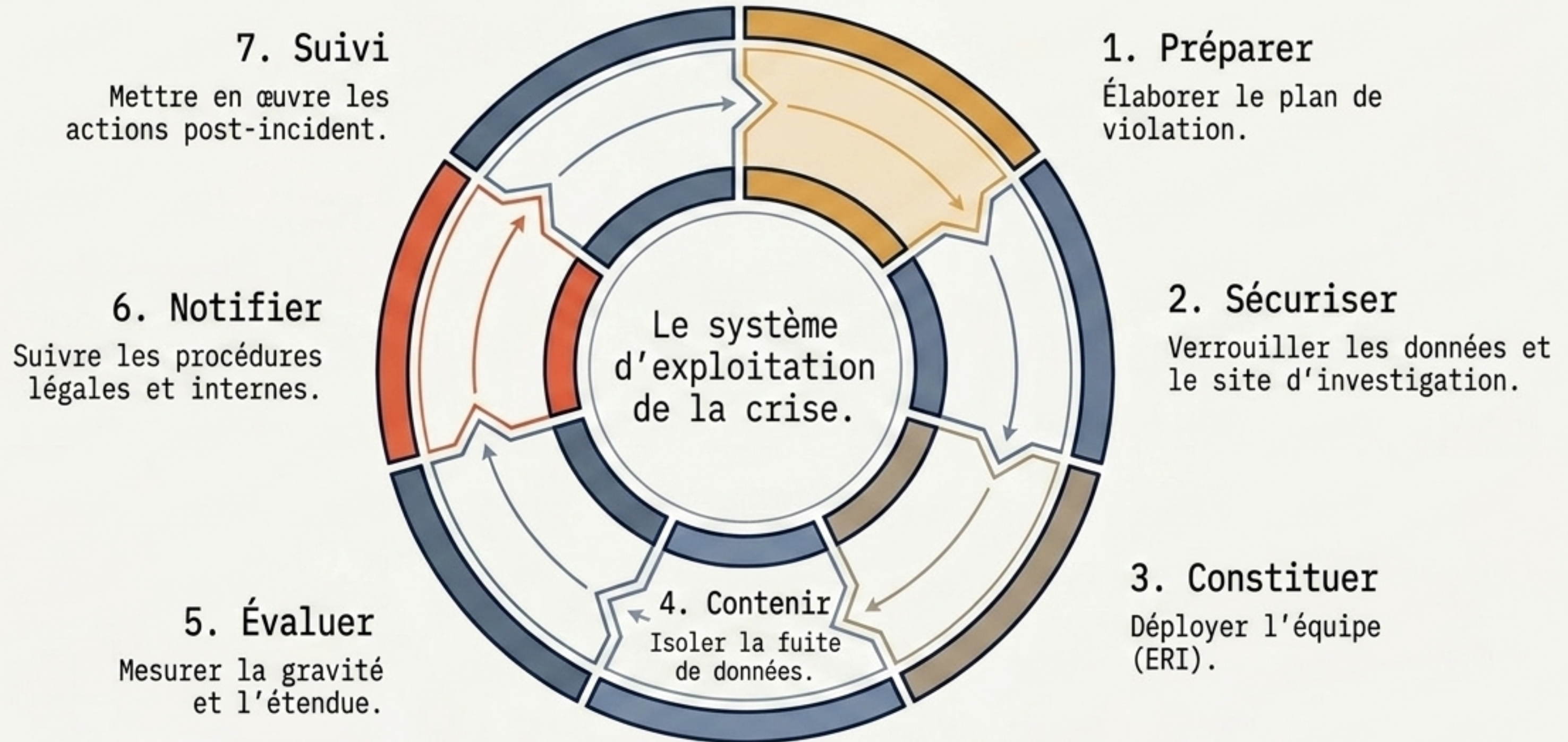


Le paradoxe opérationnel : Le CIO doit faire fonctionner l'entreprise rapidement ; le CSO doit la sécuriser. Une séparation stricte est la seule garantie d'une diligence raisonnable.

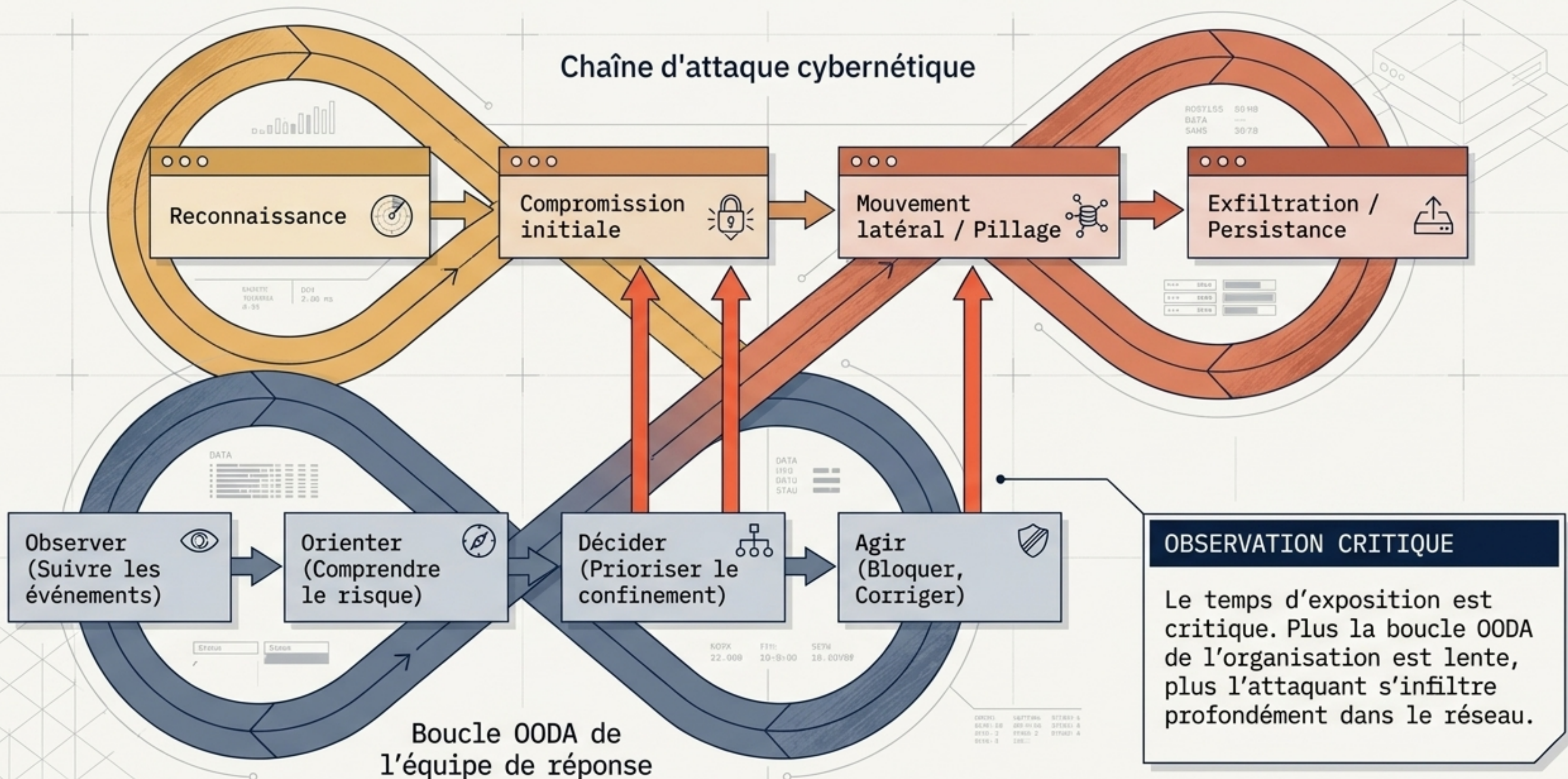
L'anatomie d'une Équipe de Réponse aux Incidents (ERI)



La méthodologie de réponse en 7 étapes



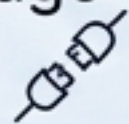
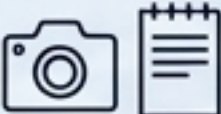
Intersection tactique : Attaquant vs Défenseur



Le paradoxe du confinement

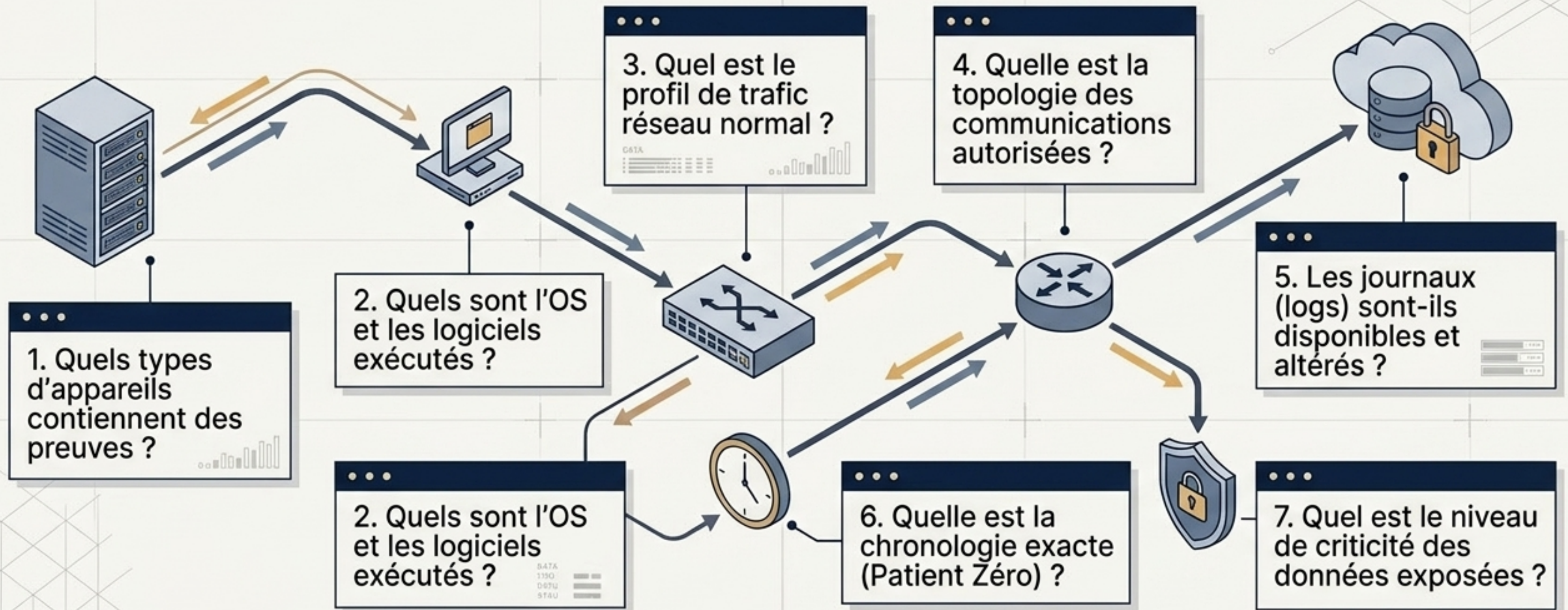
Réflexe Informatique Standard	Rigueur de la Criminalistique
Redémarrer. Effacer. Réinstaller. Détruit les preuves vitales et permet à l'attaquant de revenir en effaçant ses traces.	Isoler. Cloner. Analyser. Préserve la scène de crime numérique pour comprendre la faille et stopper les futures violations.

Les 5 règles d'or de la préservation matérielle

1. Ne pas accéder ni se connecter. 	2. Ne pas éteindre les systèmes. 	3. Isoler physiquement (débrancher, cage de Faraday). 	4. Cloner selon les normes médico-légales. 	5. Documenter et photographier tout. 
---	---	--	---	---

Évaluer l'étendue de l'incident

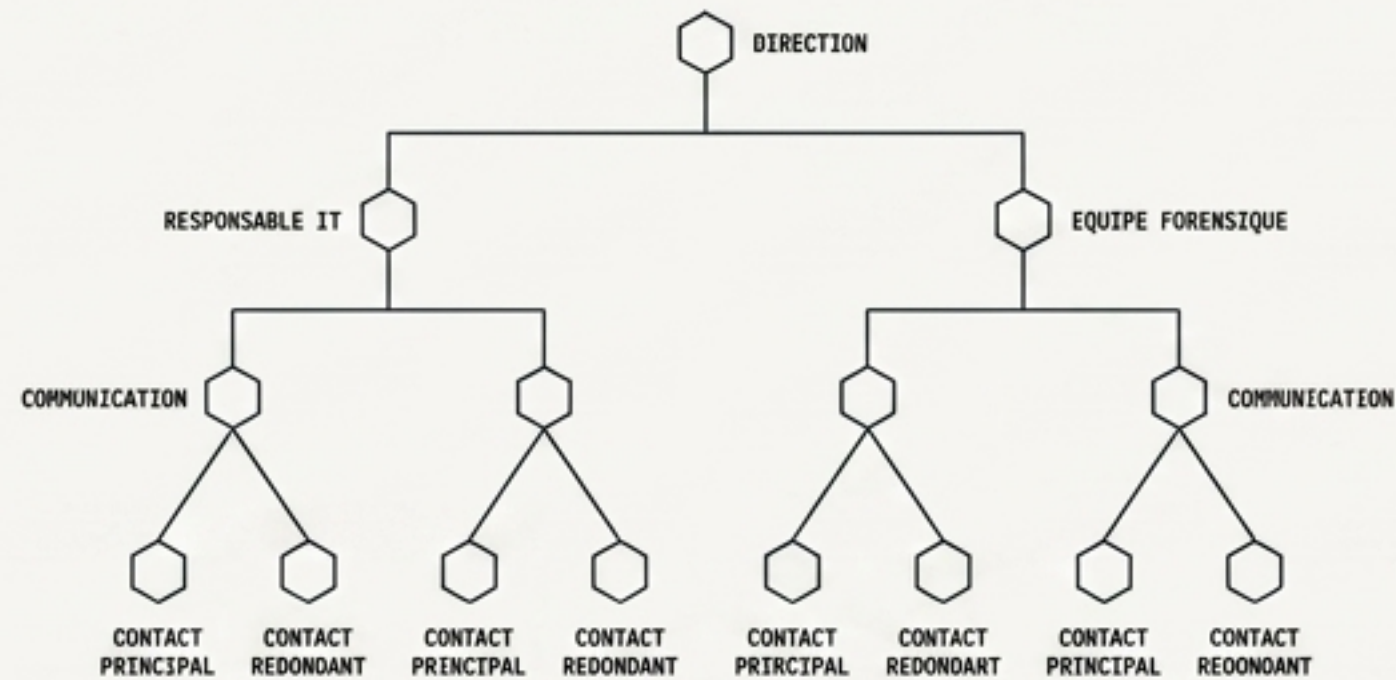
Les 7 questions diagnostiques de la criminalistique.



Les angles morts de la préparation

La logistique de crise en pleine nuit.

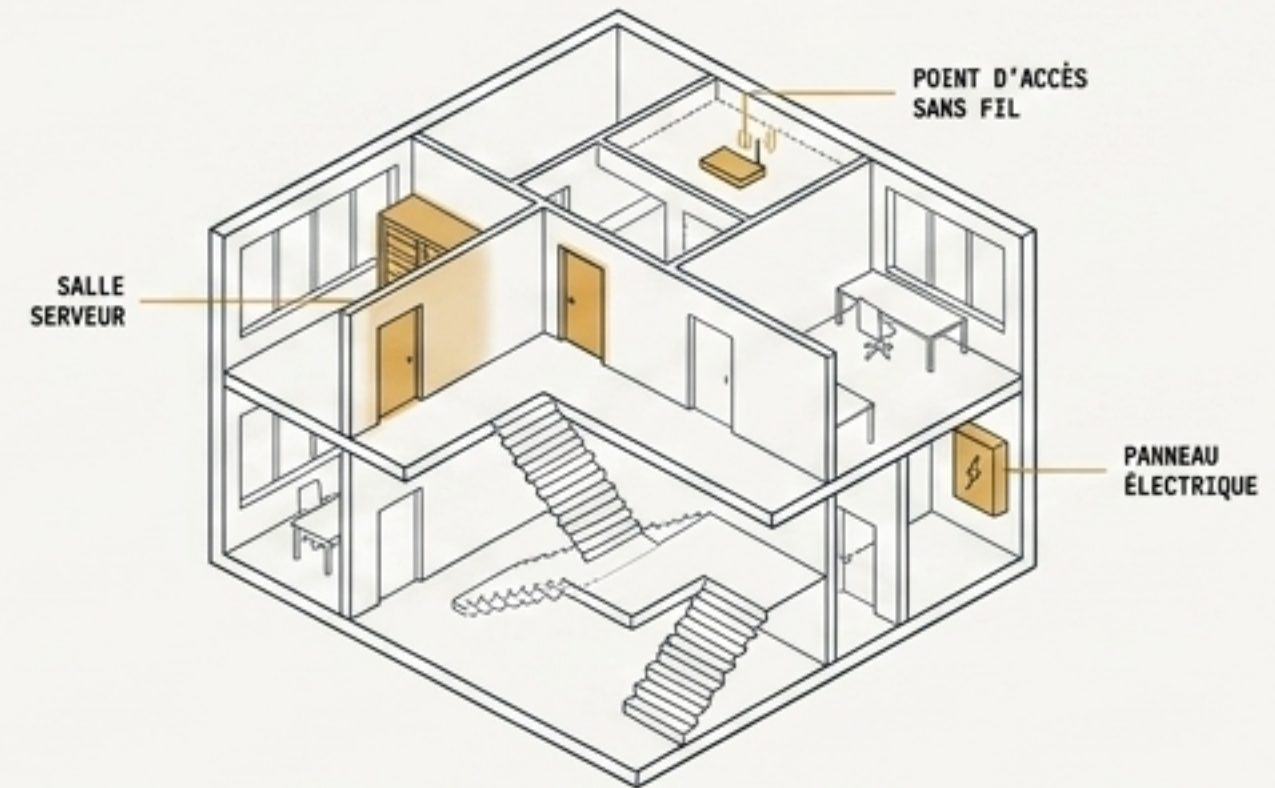
L'arborescence de communication



Le piège : Oublier les numéros complexes sous le stress. Ne pas avoir de boucle de rétroaction, laissant l'équipe submergée par les demandes de la direction.

La solution : Liste d'appels hiérarchisée, contacts redondants et un responsable de communication dédié.

L'accès aux installations physiques



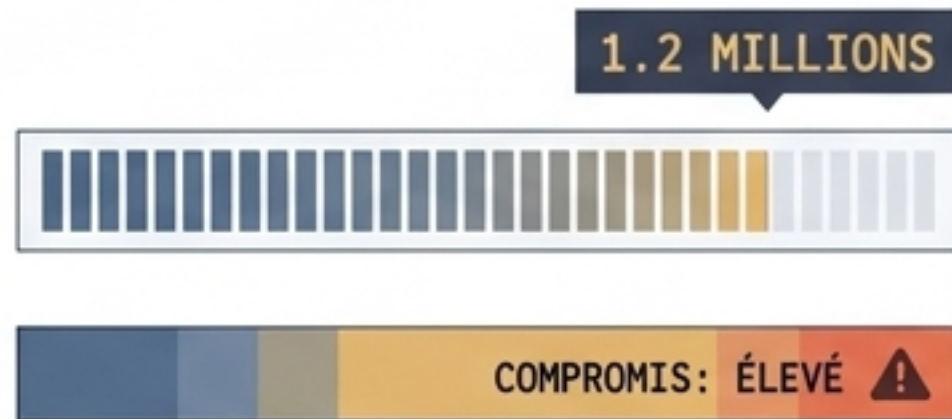
Le piège : Des enquêteurs bloqués sur le parking à 3h du matin ou incapables d'atteindre le matériel.

La solution : Accès distant pré-approuvé, logistique d'urgence (nourriture/lits 24/7) et outils de démontage physique.

Évaluer la gravité de la violation

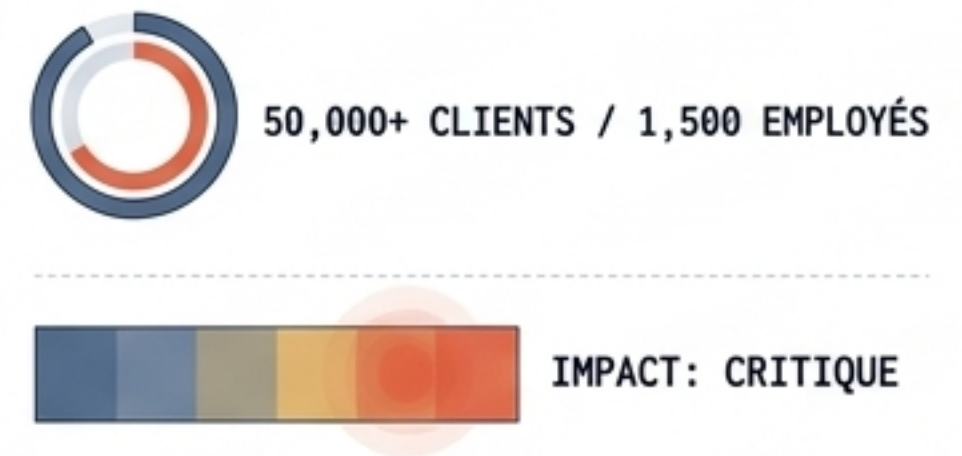
Volume

Nombre total d'enregistrements volés ou compromis



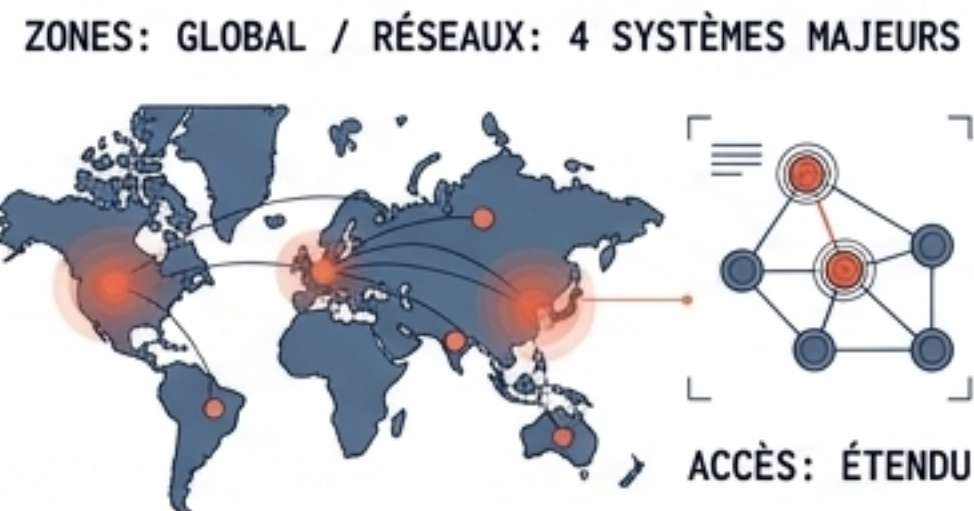
Impact Humain

Nombre de clients et d'employés directement affectés



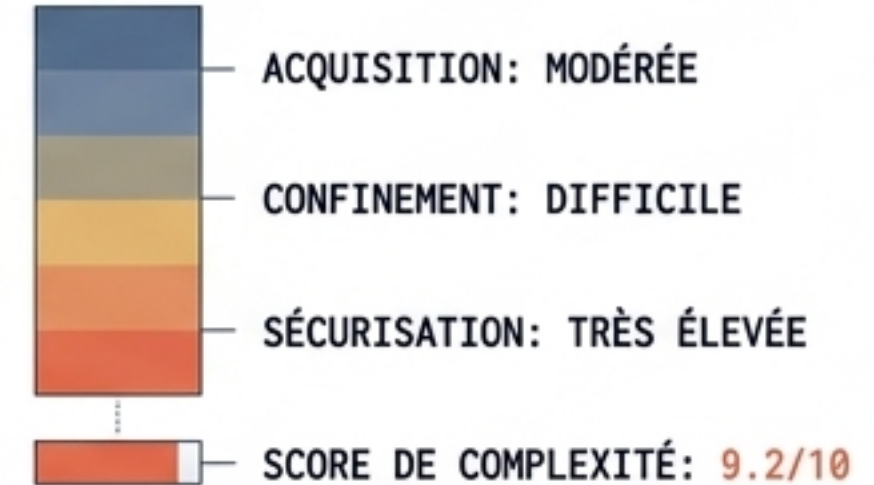
Empreinte

Zones géographiques et réseaux touchés



Complexité

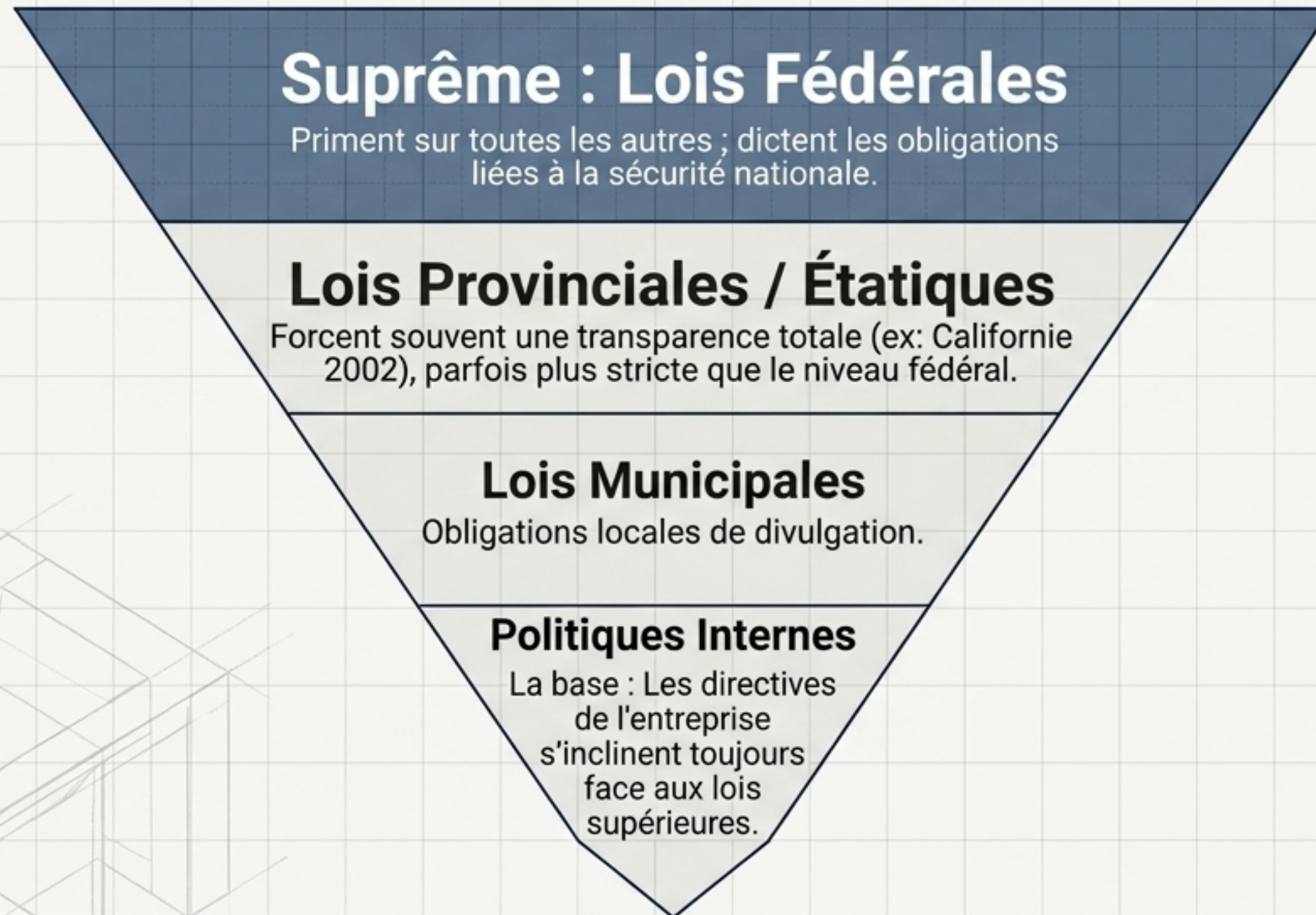
Difficulté d'acquisition, de confinement et de sécurisation



L'évaluation abstraite de la valeur

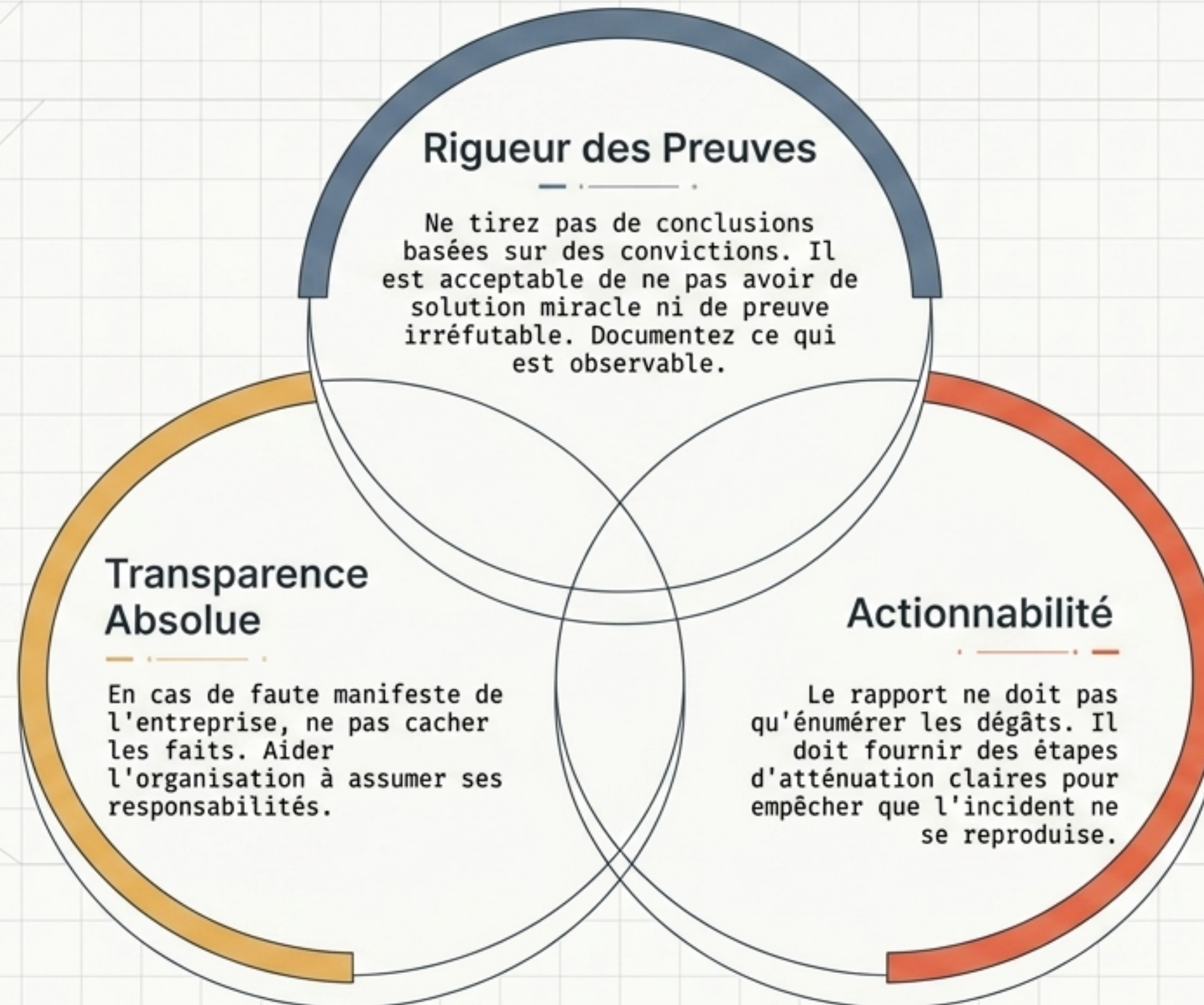
Le coût dépasse le simple vol de cartes de crédit. L'attaque contre **Sony Pictures (2014)** a touché peu d'enregistrements purs, mais a forcé l'annulation de la sortie d'un film, causant des pertes de **plusieurs millions de dollars**.

La hiérarchie des notifications légales

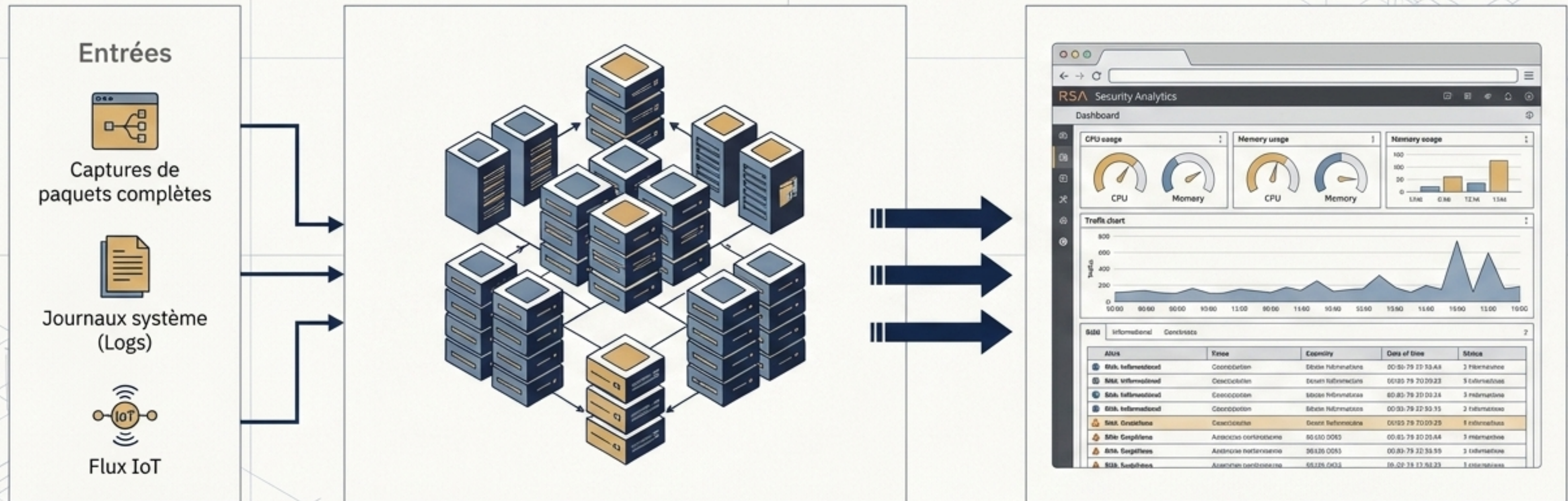


Le paradoxe de la divulgation : Par obligation enquêteurs doivent souvent adopter une approche cumulative et transparente, divulguant parfois des systèmes potentiellement compromis même sans preuves irréfutables.

L'éthique du rapport post-incident



L'architecture de sécurité (SIEM & Big Data)



Entrées

Moteur : Clusters Big Data Hadoop

Interrogeables de manière rétroactive
(Ex: RSA Security Analytics, QRadar).

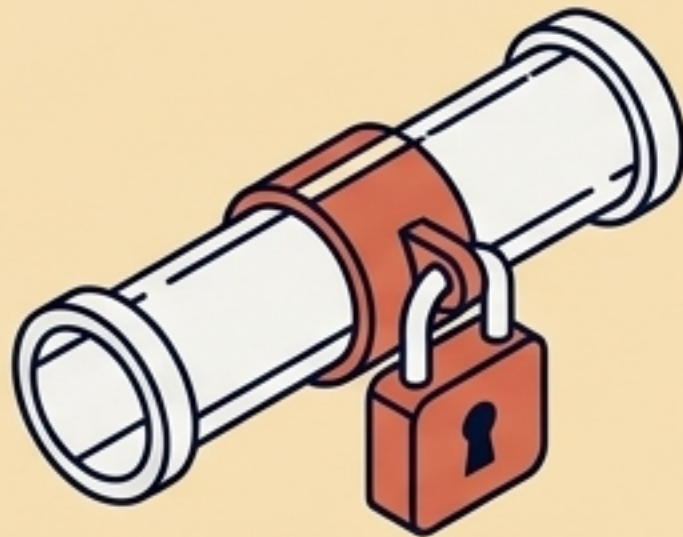
Fonction : Rejouer & Corréler

Permet de rejouer l'intégralité d'une session de trafic et d'examiner le contenu exact des fuites de données.

Analyse des tendances et défis futurs

Filtrer le bruit

Utilisation d'outils comme NetFlow, SolarWinds, ou Splunk pour filtrer les millions de logs et identifier les anomalies comportementales via des cartes, graphiques et arborescences.



Le défi ultime : Le trafic chiffré

L'angle mort : Les attaques modernes se cachent dans le chiffrement (SSL).

Solutions complexes : Interception SSL, attaques Homme du Milieu contrôlées, ou analyses de métadonnées (Cisco ETA).

La technologie donne la visibilité, mais seule une gouvernance rigoureuse et une équipe entraînée peuvent refermer la boucle OODA.