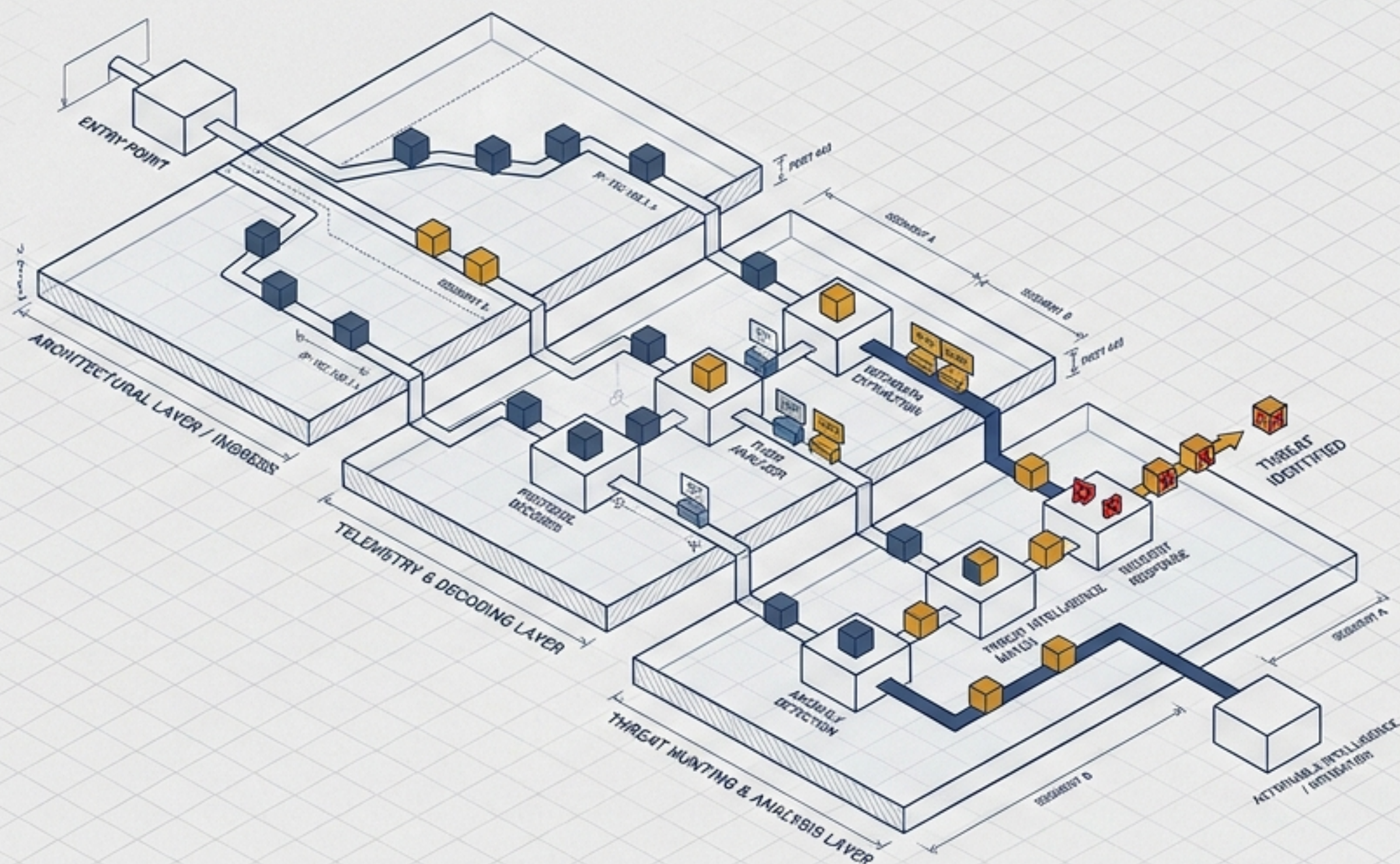


Analyse forensique des réseaux

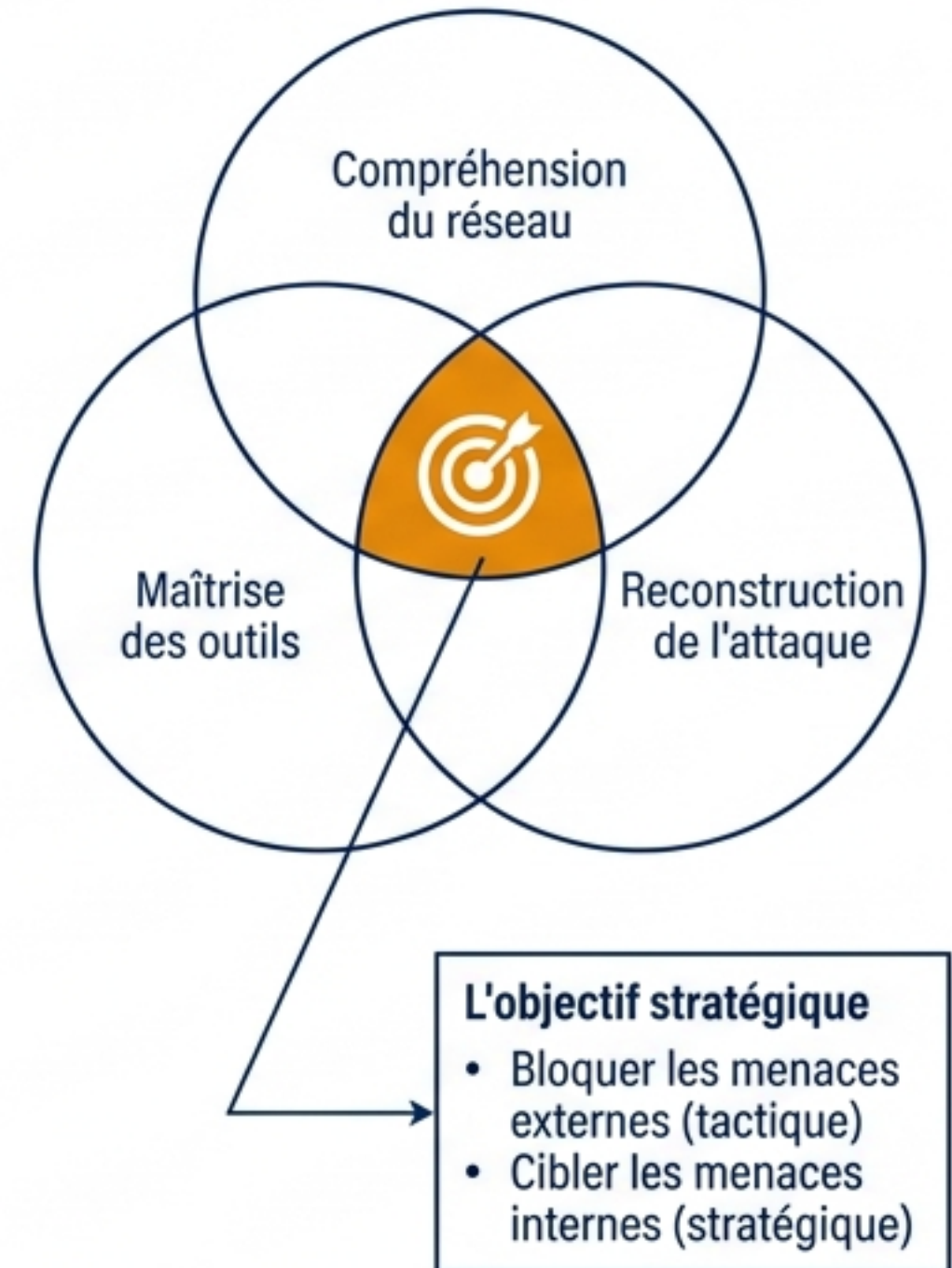
Cartographier l'architecture, décoder la télémétrie et chasser les menaces.



« L'espoir est la dernière chose qu'une personne fait avant d'être vaincue. »

— Henry Rollins

L'intersection forensique



L'expertise réside dans la reconstitution intégrale de l'événement, bien au-delà des alertes automatisées.

L'ADN du trafic : Identifier les portes d'entrée

Sur 65 535 ports disponibles, l'analyste doit maîtriser instantanément les ports critiques de la couche transport.



TCP (Fiabilité garantie)

Connexion directe, livraison certifiée.

Exemple : FTP (Ports 20/21).



UDP (Livraison sans garantie)

Rapide, dépend des intermédiaires, aucune confirmation.

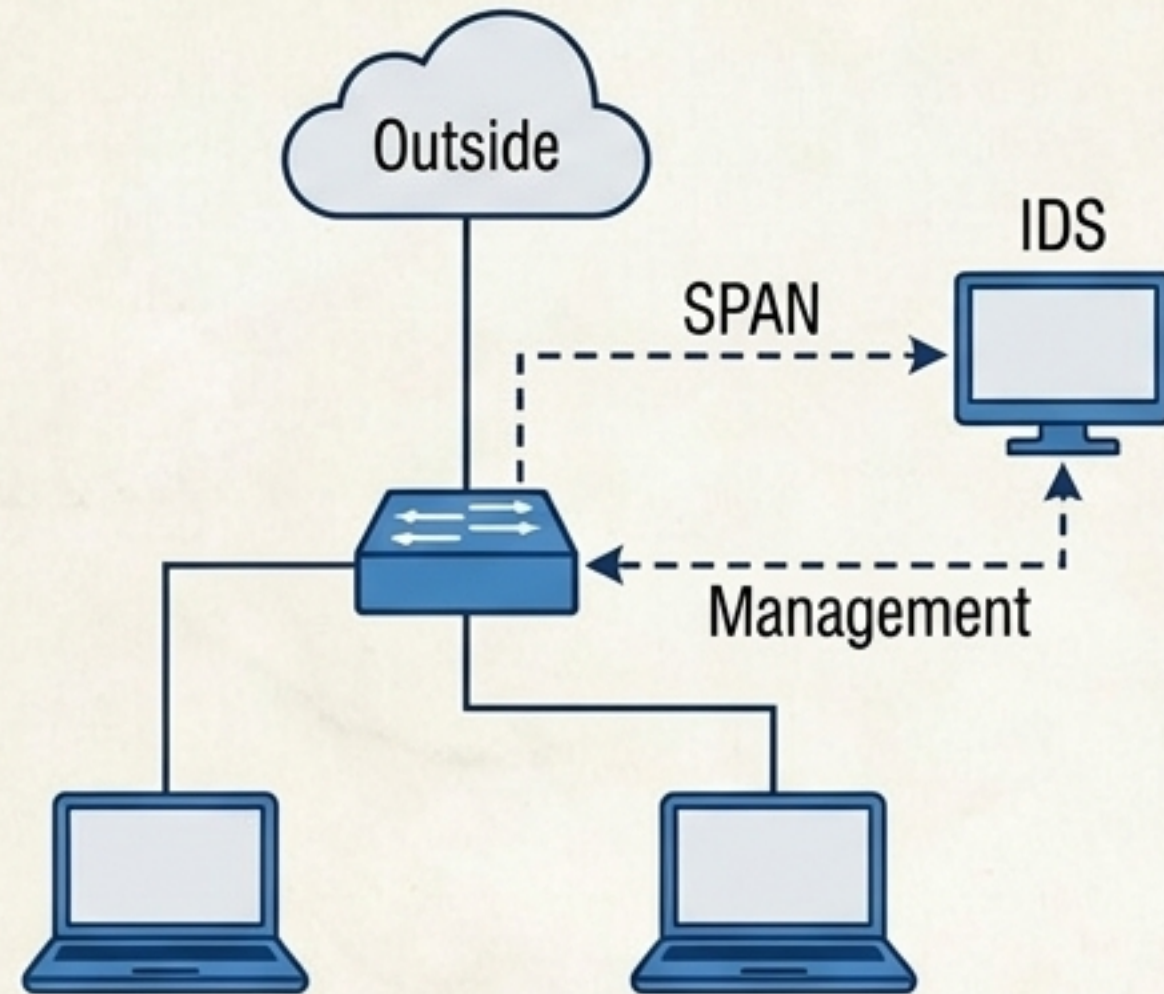
Exemple : DNS (Port 53).

--- AIDE-MÉMOIRE IANA ---

[21]	FTP	[80]	HTTP
[22]	SSH	[110]	POP3
[23]	Telnet	[119]	NNTP
[25]	SMTP	[123]	NTP
[53]	DNS	[143]	IMAP
[161]	SNMP	[443]	HTTPS
[194]	IRC		

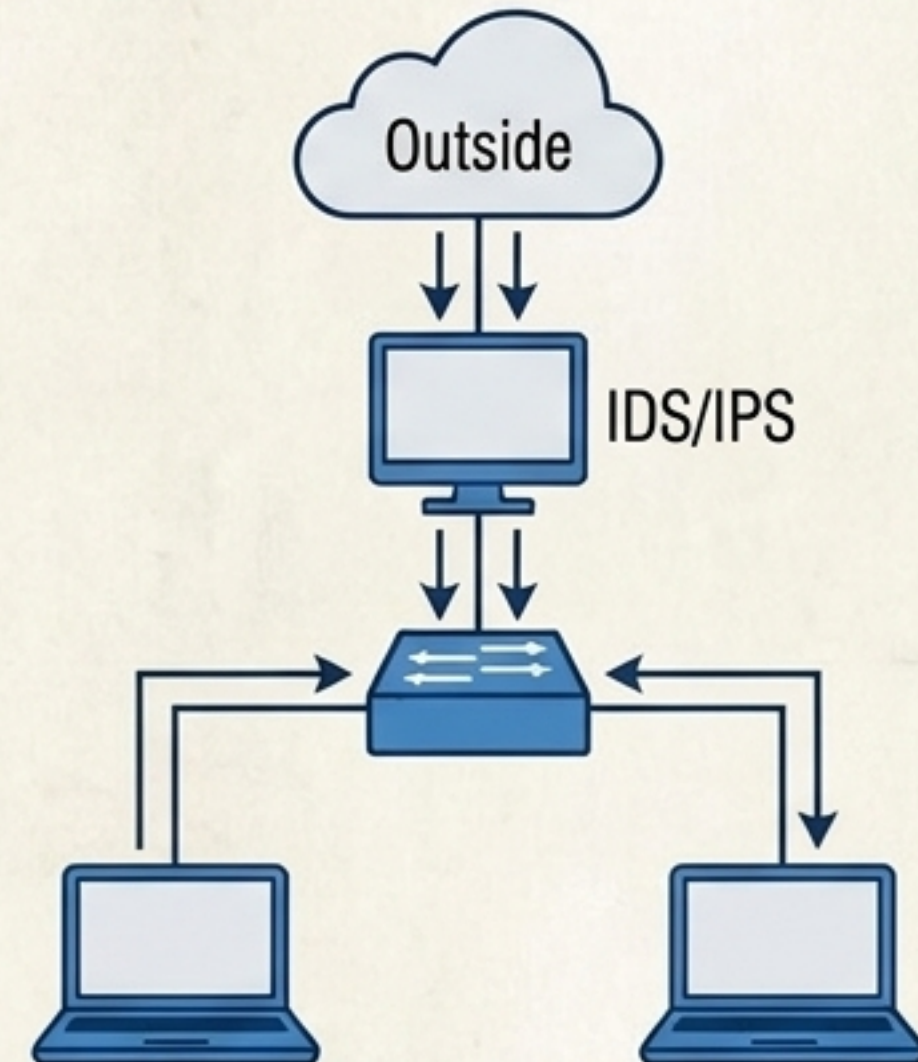
Topologie de déploiement : L'emplacement dicte l'action

Déploiement Passif (Observation)



Avantage : Zéro latence, aucune interruption réseau.
Limite : Incapable d'interrompre une connexion en direct sans aide externe.

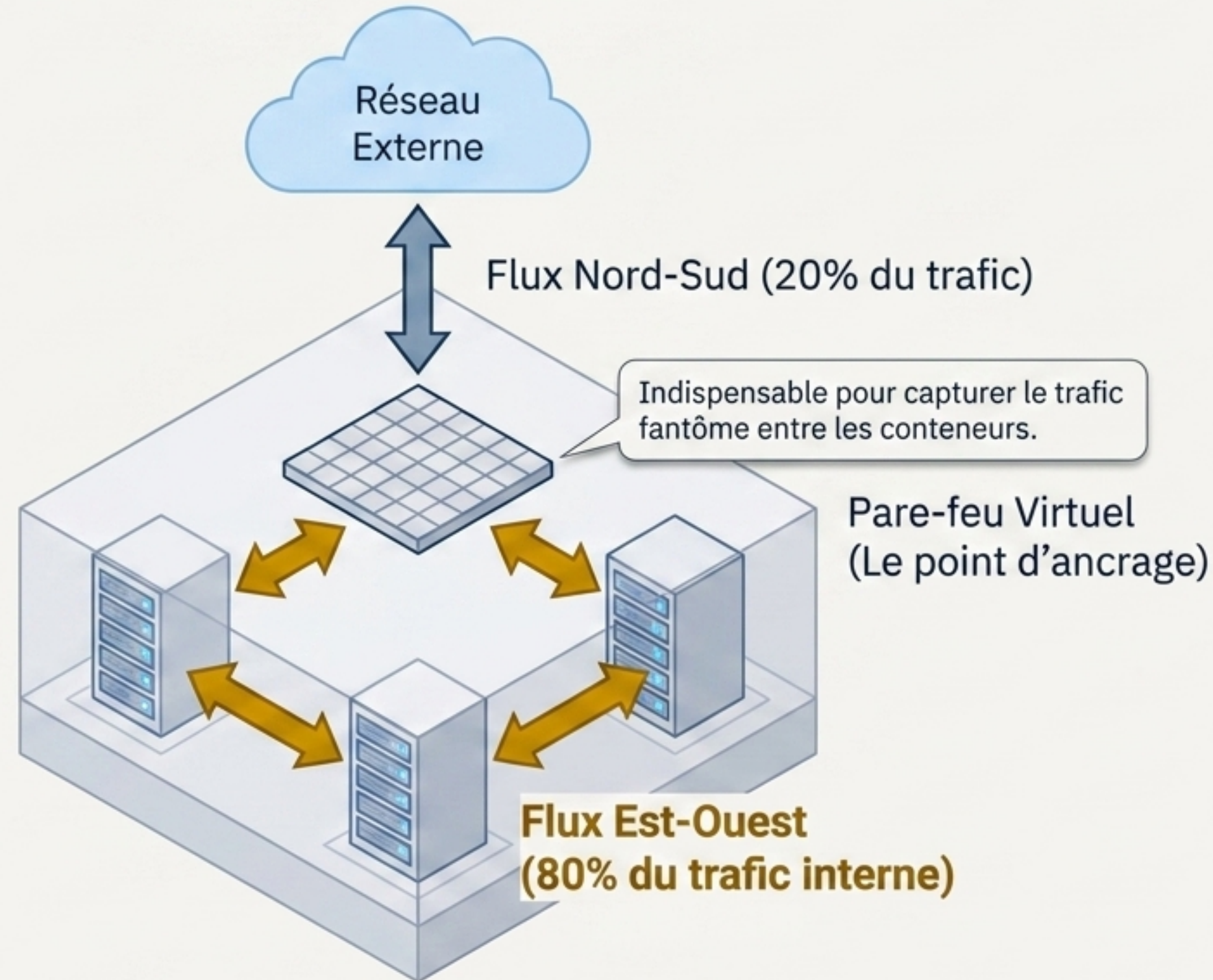
Déploiement En Ligne (Intervention)



Avantage : Action immédiate (ex: réinitialisation TCP).
Limite : Crée un goulot d'étranglement matériel.

La frontière virtuelle : Les angles morts du centre de données

Sécuriser uniquement le périmètre rend aveugle aux menaces internes (SDN et Conteneurs).



Segmentation et Topographie de la Confiance

L'investigation s'appuie sur la violation des limites logiques et physiques.

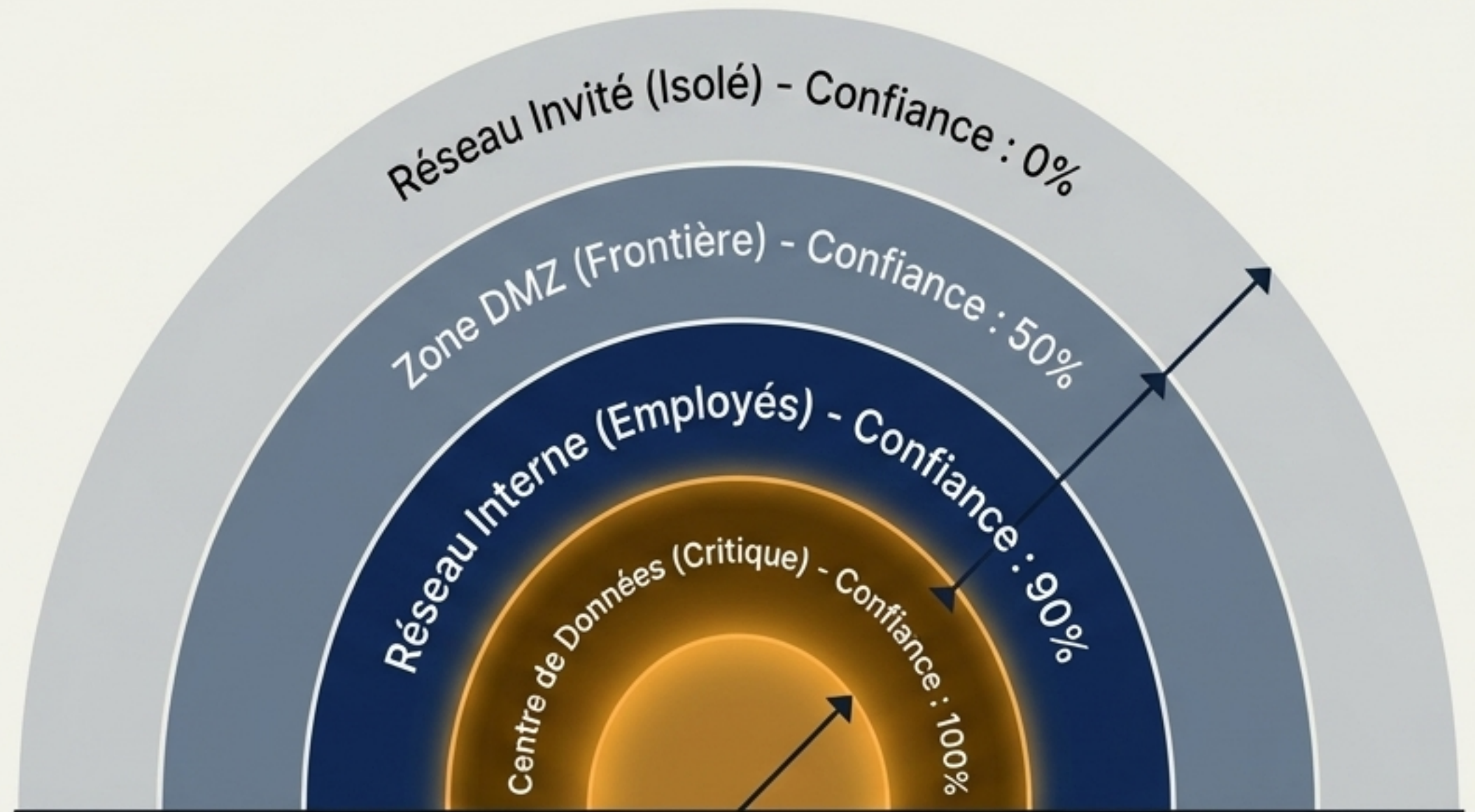
Séparation Physique

Contextes de Pare-feu

VLAN (Réseaux Virtuels)

ACL (Listes de Contrôle)

SGT (Étiquettes de Groupe)



L'Arsenal Périphérique : Matrice d'extraction de données

	Pare-feu (Next-Gen)	Filtre de Contenu / Proxy	Contrôle d'Accès (NAC)																																
Emplacement & Mécanisme	Périphérie. Validation de l'état du réseau.	Proxys Web (WCCP) et Pare-feu applicatif.	Protocoles 802.1x et SNMP. Authentification.																																
Trace Forensique	IP sources/destinations, ports et services franchissant la zone.	Sécurité par réputation, requêtes web mises en cache, déclencheurs DLP.	Identité de l'appareil, profil, et horodatage de connexion.																																
Le Super-Pouvoir	Détection des flux externes.		Le Contexte : Transforme une IP anonyme en identité. <table><thead><tr><th>Time</th><th>Details</th><th>Identity</th><th>Endpoint ID</th></tr></thead><tbody><tr><td></td><td></td><td> </td><td> </td></tr><tr><td>Aug 08, 2017 PM</td><td></td><td>00:11:8B EA.E9.12</td><td>00:11:8B EA.E9.12</td></tr><tr><td>Aug 08, 2017 PM</td><td></td><td>00:11.8B.C2.E4:56</td><td>00:11:8B.C2.E4:56</td></tr><tr><td>Aug 08, 2017 PM</td><td></td><td>mantirabe</td><td>EB:E5:E5:D6.70:DE...</td></tr><tr><td>Aug 08, 2017 PM</td><td></td><td>contractor087</td><td>CC:07:E4:C3.79:...</td></tr><tr><td>Aug 08, 2017 PM</td><td></td><td>contractor087</td><td>CC:07:E4:C3.79:...</td></tr><tr><td>Aug 08, 2017 PM</td><td></td><td>adio</td><td>A8:20:66:58:85:D6</td></tr></tbody></table>	Time	Details	Identity	Endpoint ID					Aug 08, 2017 PM		00:11:8B EA.E9.12	00:11:8B EA.E9.12	Aug 08, 2017 PM		00:11.8B.C2.E4:56	00:11:8B.C2.E4:56	Aug 08, 2017 PM		mantirabe	EB:E5:E5:D6.70:DE...	Aug 08, 2017 PM		contractor087	CC:07:E4:C3.79:...	Aug 08, 2017 PM		contractor087	CC:07:E4:C3.79:...	Aug 08, 2017 PM		adio	A8:20:66:58:85:D6
Time	Details	Identity	Endpoint ID																																
Aug 08, 2017 PM		00:11:8B EA.E9.12	00:11:8B EA.E9.12																																
Aug 08, 2017 PM		00:11.8B.C2.E4:56	00:11:8B.C2.E4:56																																
Aug 08, 2017 PM		mantirabe	EB:E5:E5:D6.70:DE...																																
Aug 08, 2017 PM		contractor087	CC:07:E4:C3.79:...																																
Aug 08, 2017 PM		contractor087	CC:07:E4:C3.79:...																																
Aug 08, 2017 PM		adio	A8:20:66:58:85:D6																																

L'Arsenal Intelligent : Détection et Tromperie

1. IDS / IPS

- Détection par signature (vulnérabilités connues).
- Analyse comportementale (anomalies de trafic).
- Nécessite des mises à jour constantes.

2. Bac à Sable (Sandbox)

- Détonation contrôlée de fichiers non fiables.
- Capture des hachages et modifications du registre.

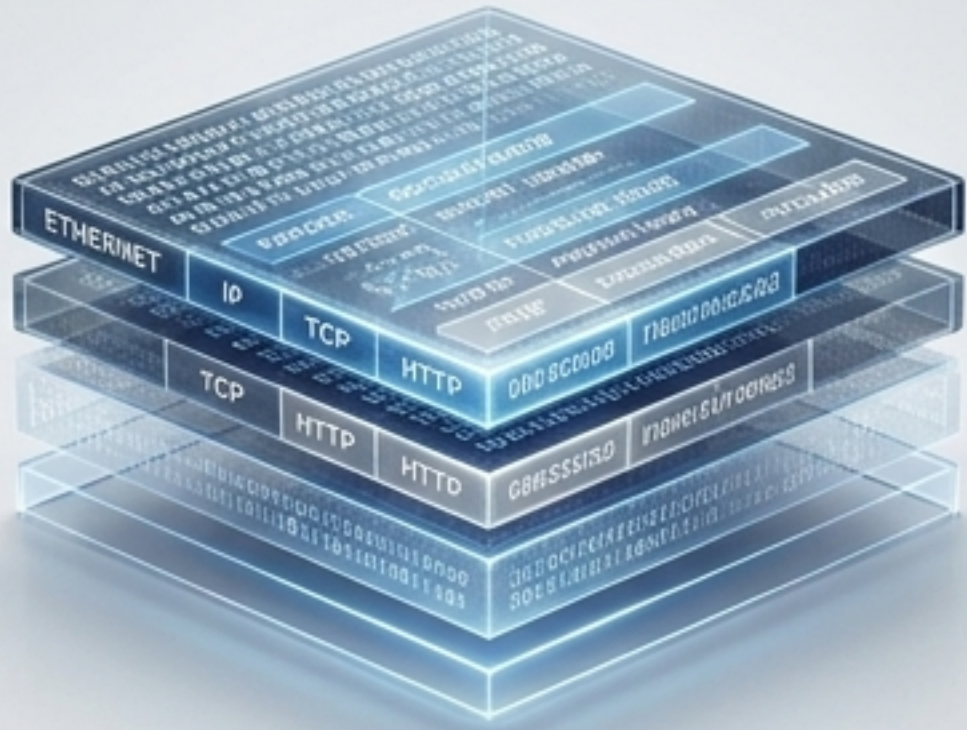


3. Pot de Miel (Honeypot)

- Système leurre hautement vulnérable.
- Zéro faux positif : toute interaction est suspecte.
- Capture l'intention et les outils de l'attaquant.

Le Grand Débat Télémétrique : PCAP vs NetFlow

PCAP (Capture de Paquets)



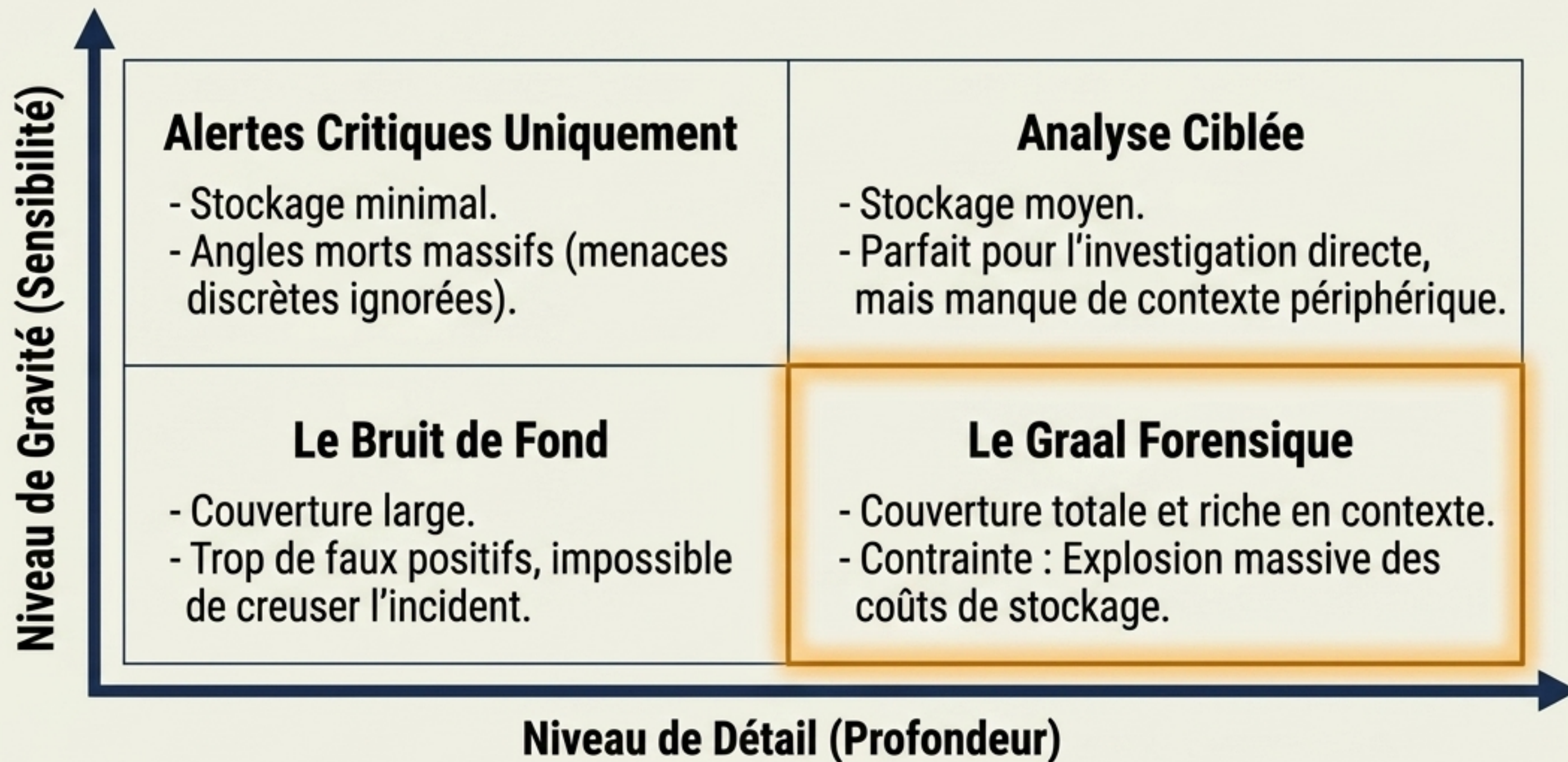
- **Métaphore** : L'enregistrement vidéo HD de l'événement.
- Preuve absolue et relecture exacte de bout en bout.
- Contraintes : Très coûteux en stockage, aveugle face au trafic chiffré.

NetFlow (Analyse de Flux)



- **Métaphore** : La facture de téléphone détaillée (Qui, Quand, Durée).
- Léger, idéal pour établir des lignes de base (**baselines**) comportementales.
- **Piège** : La déduplication des enregistrements peut corrompre la piste forensique.

Stratégie de Journalisation : Visibilité vs Stockage



Cycle de vie : Stockage local (rapide, 30-90 jours) -> Export externe (compressé, nécessite réhydratation)

Décoder les Traces : Extraction en Ligne de Commande

Standardisation Syslog (CEF vs LEEF)

CEF:0|Trend Micro|...|**suser=Administrateur**|...

LEEF:2.0|Trend Micro|...|**usrName=Systeme**|...

Attention aux clés
d'utilisateur distinctes
selon le format.

L'Arsenal d'Extraction Linux

grep -B 3 -A 2 'Invalid user' **/var/log/auth.log**

Recherche avec contexte
(-B avant, -A après)

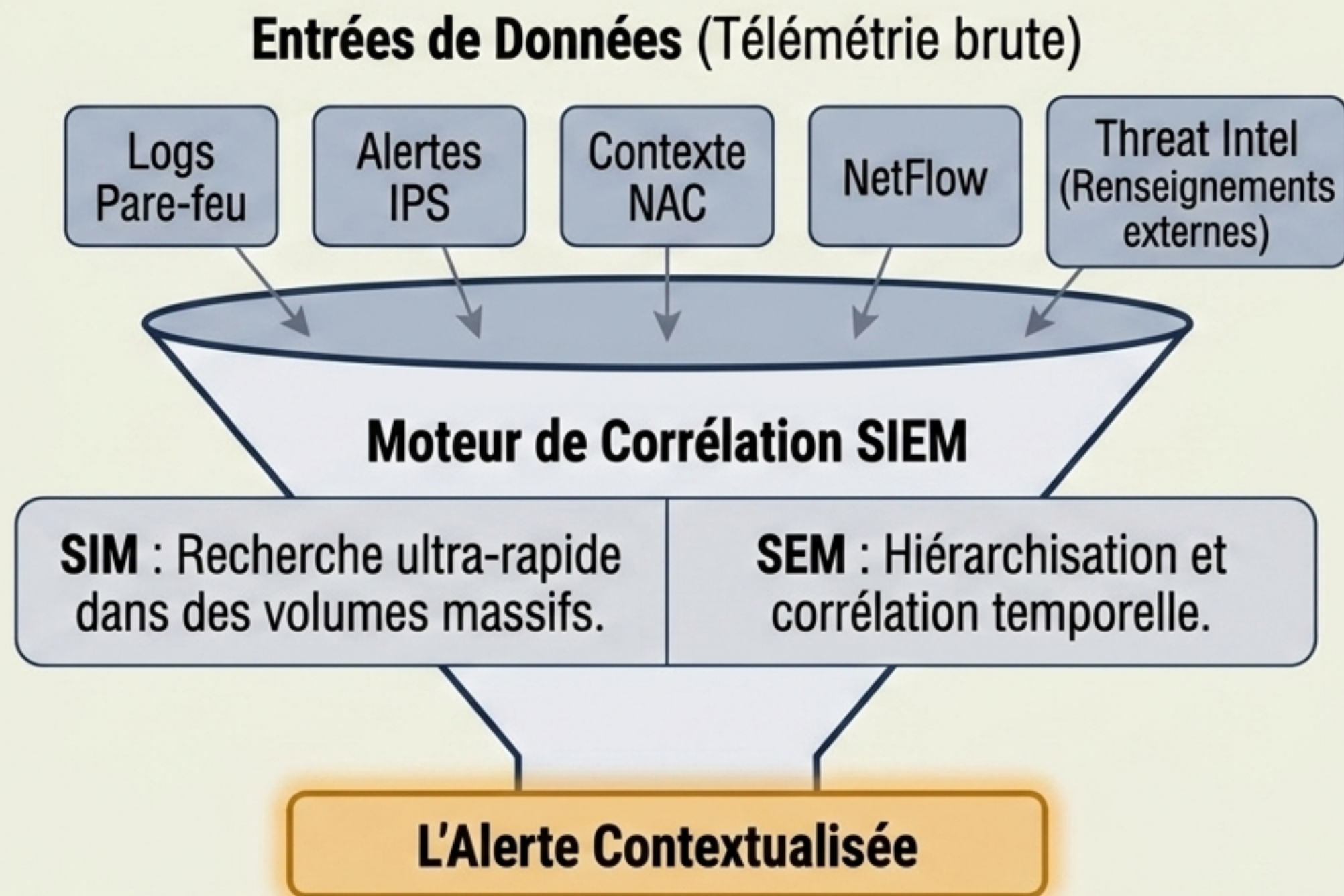
grep 'authentication failure' **auth.log** | cut -d '=' -f 6

Séparation par délimiteurs
(isole la 6^{ème} valeur après '=')

awk '/sshd.*utilisateur invalide/ {print \$9}' **auth.log**

Filtrage avancé et extraction
de colonnes par Regex

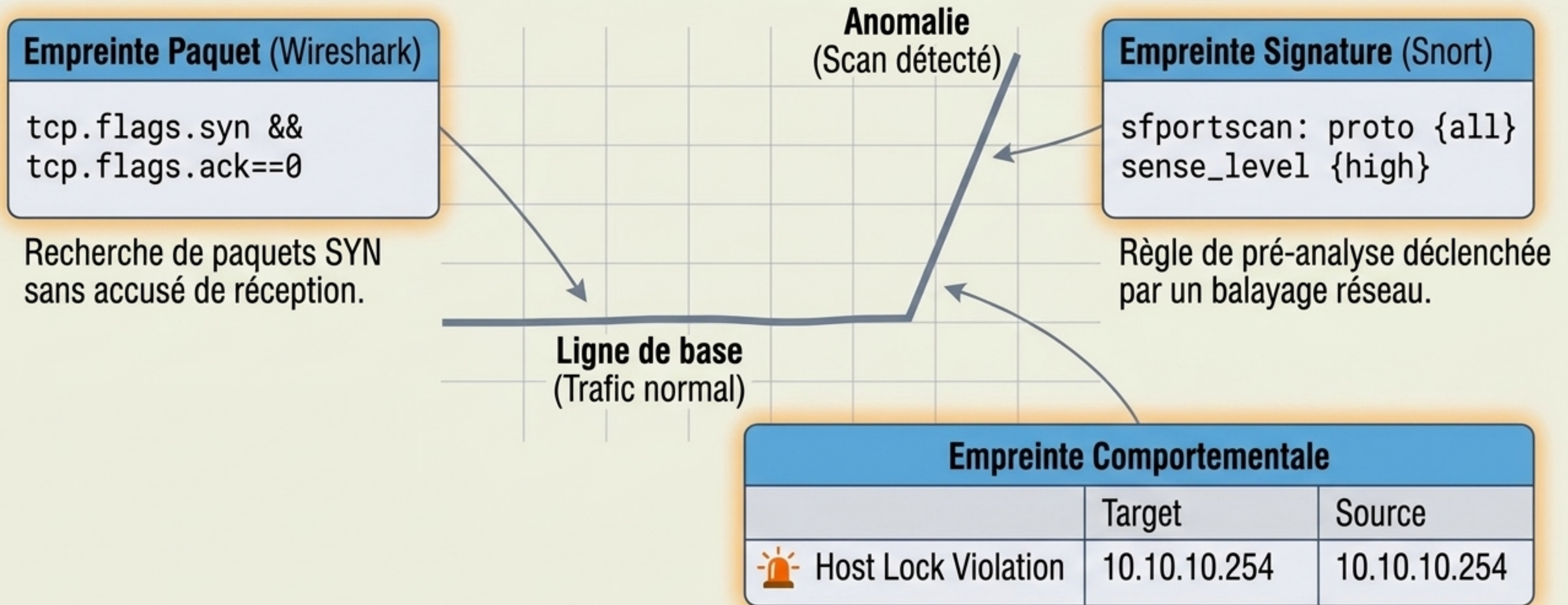
Le Cerveau Opérationnel : SIEM et Renseignement



Une chronologie d'attaque unique, priorisée et enrichie de signatures externes pour une remédiation proactive.

Chasser l'Invisible : Identifier la Reconnaissance

La première phase de la Kill Chain trahit l'attaquant par des déviations de la ligne de base.



Alerte de Verrouillage d'hôte suite à une déviation de protocole.

Synthèse : L'Écosystème Forensique Interconnecté



**L'investigation n'est pas la lecture d'un seul outil,
c'est l'art de relier des fragments d'architecture.**