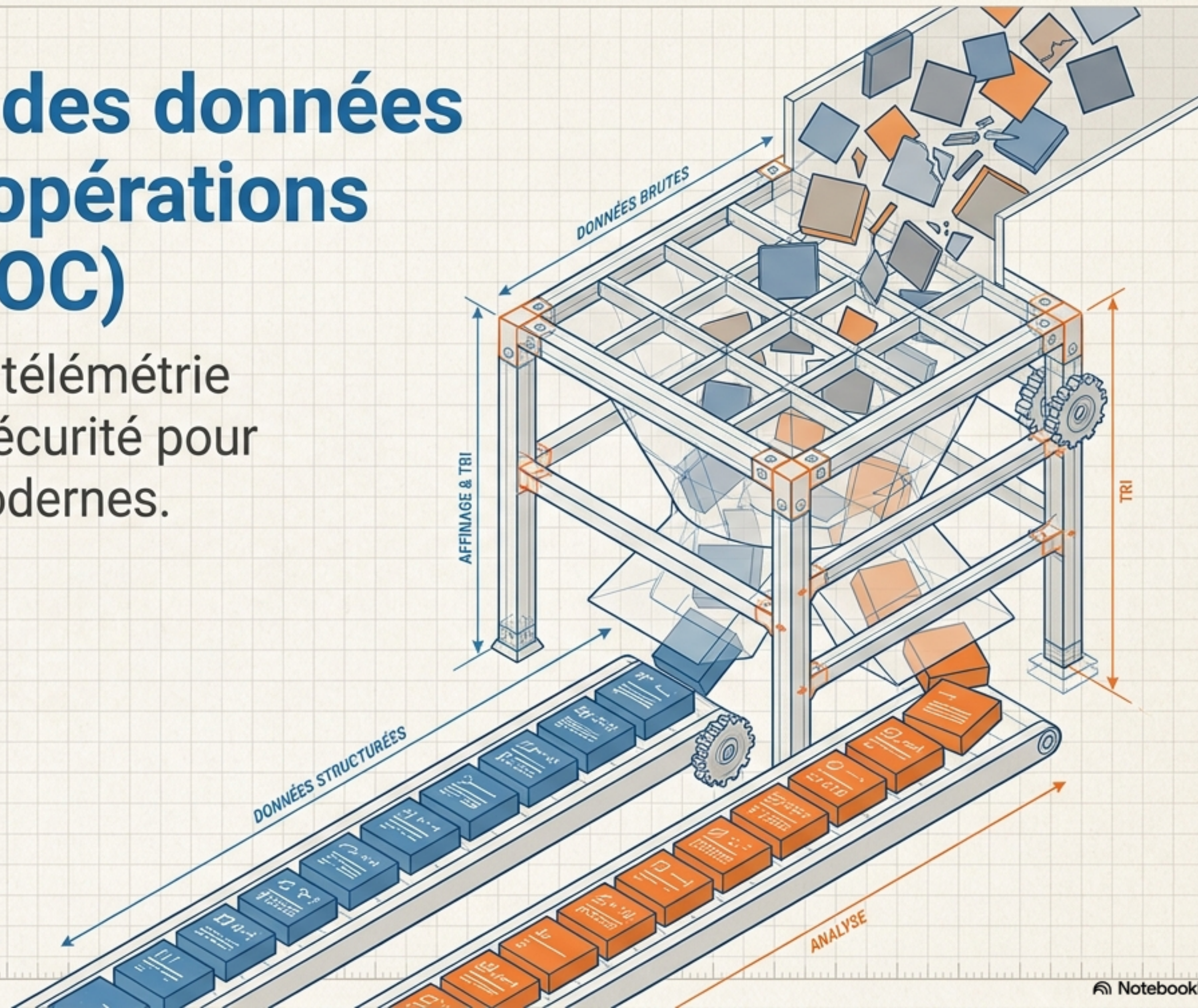
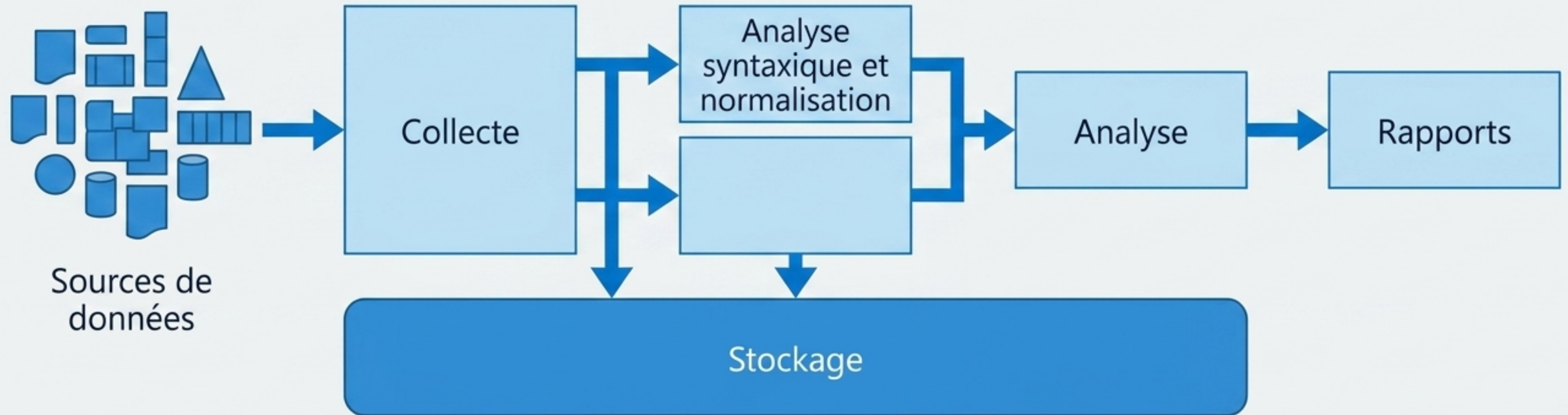


L'architecture des données d'un Centre d'opérations de sécurité (SOC)

Stratégies de collecte, télémétrie réseau et analyse de sécurité pour les environnements modernes.



Avant toute analyse utile, il est indispensable d'acquérir les données pertinentes



Les données non structurées n'ont aucune valeur d'investigation sans ce cycle de vie rigoureux.

L'objectif n'est pas de tout surveiller, mais d'éliminer les angles morts stratégiques



Périmètre

Quels éléments nécessitent une surveillance active ?



Format

Quelles données collecter et selon quel protocole ?



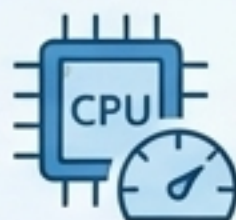
Profondeur

Quel niveau de journalisation est requis par appareil ?



Rétention

Combien de temps conserver les données pour la conformité ?



Impact

Quelle est la charge induite sur le processeur et le réseau ?

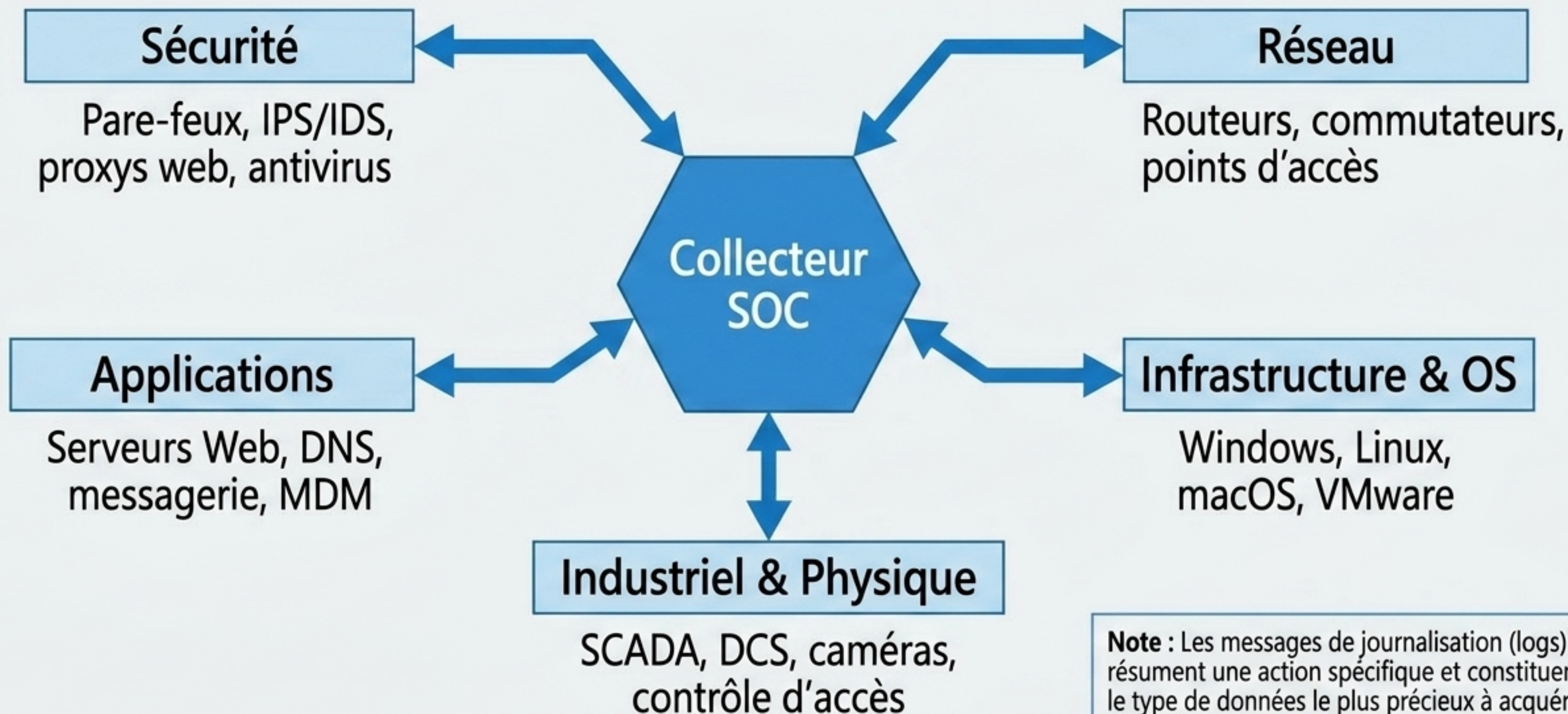


Capacité

Comment optimiser le stockage et le traitement ?

De nombreuses défaillances de SOC proviennent de mauvaises pratiques de collecte : angles morts, manque de corrélation, ou simple absence de synchronisation temporelle.

L'écosystème des sources de données de sécurité couvre l'ensemble de l'infrastructure



Le standard de journalisation de l'industrie repose sur l'architecture Syslog (RFC 5424)

Le Collecteur (Collector)

Reçoit et stocke les événements centralisés

Le Relais (Relay)

Reçoit et réplique les messages pour limiter la charge sur les émetteurs

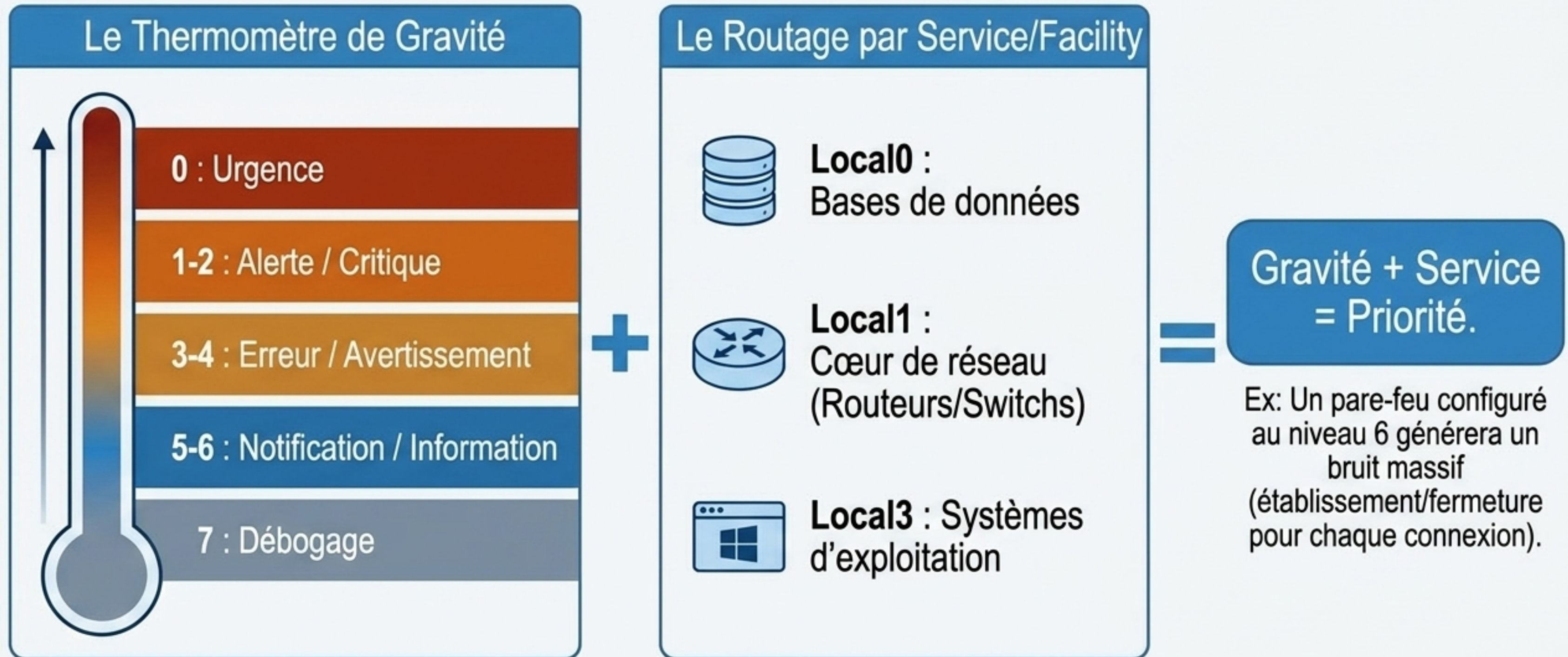
L'Émetteur (Originator)

Génère le contenu Syslog (pare-feux, serveurs)



Syslog utilise UDP/514 par défaut (aucune sécurité native). Pour les environnements sécurisés, l'encapsulation via TLS ou DTLS (RFC 5425) est impérative.

La priorité d'un événement est calculée par la combinaison de sa gravité et de son service d'origine

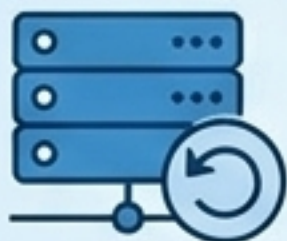


Sécuriser et optimiser l'infrastructure de journalisation



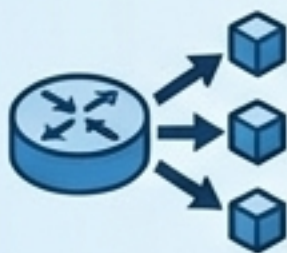
Synchronisation NTP absolue

La journalisation sans horodatage précis via un serveur NTP corrompt toute enquête forensique future.



Redondance locale

Maintenir un cache local en cas de panne réseau empêchant l'accès au collecteur.



Limitation des collecteurs

Utiliser des relais syslog pour répliquer un événement vers plusieurs équipes plutôt que de surcharger le client.



Surveillance de la surcharge (EPS)

Établir une ligne de base des Événements Par Seconde (EPS) pour anticiper l'impact sur le CPU et la bande passante.



Protection des archives

Accès en lecture seule strictement limité ; **rotation et chiffrement** appliqués au référentiel.

Au-delà des journaux : le réseau entier devient un capteur avec IPFIX et NetFlow

Qu'est-ce qu'un flux ?

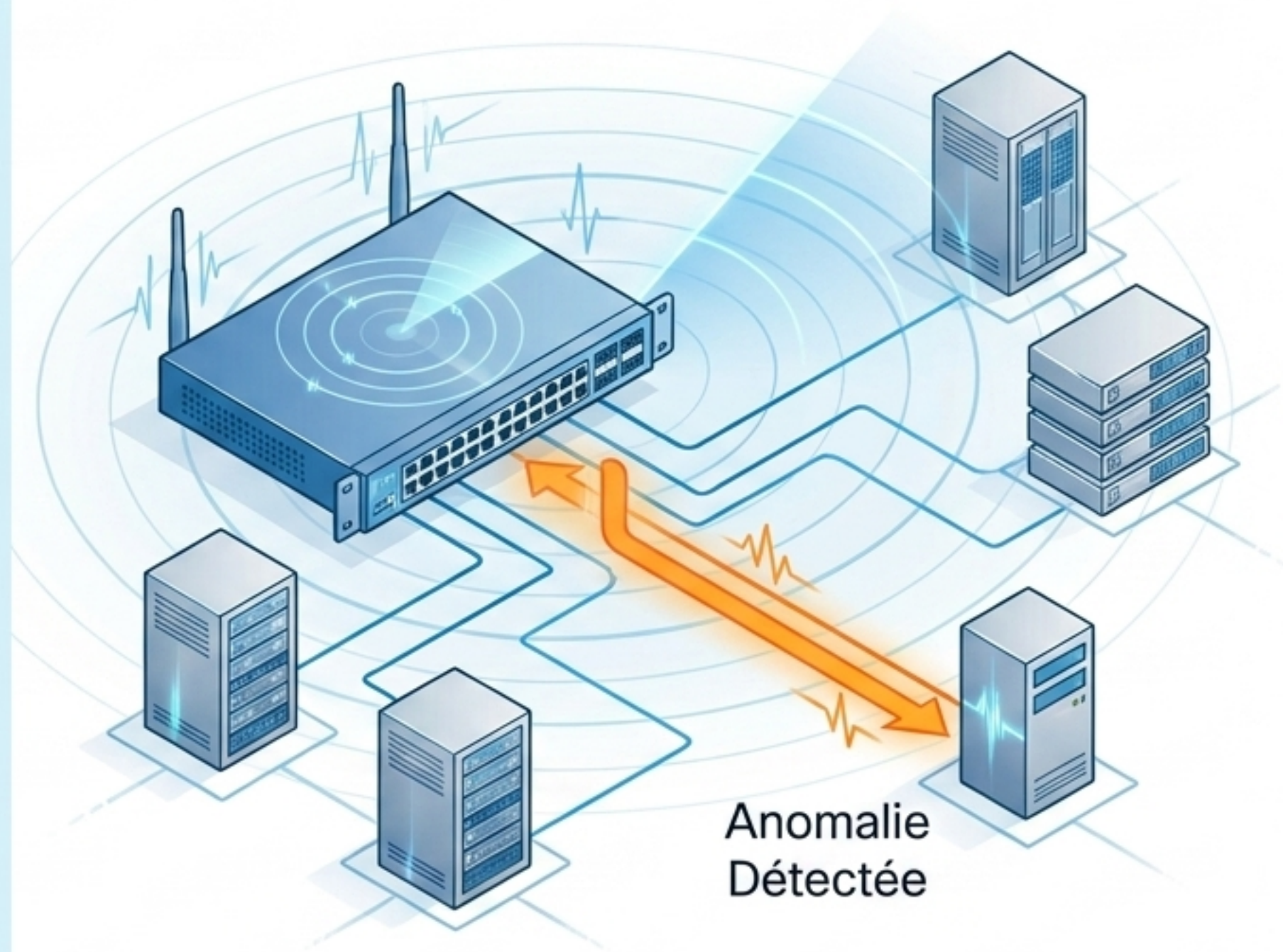
Une série de paquets partageant les mêmes attributs durant un intervalle (IP source/dest, ports, protocole).

Normes :

Cisco NetFlow v9 et la norme ouverte IPFIX (UDP/4379, TCP/4379).

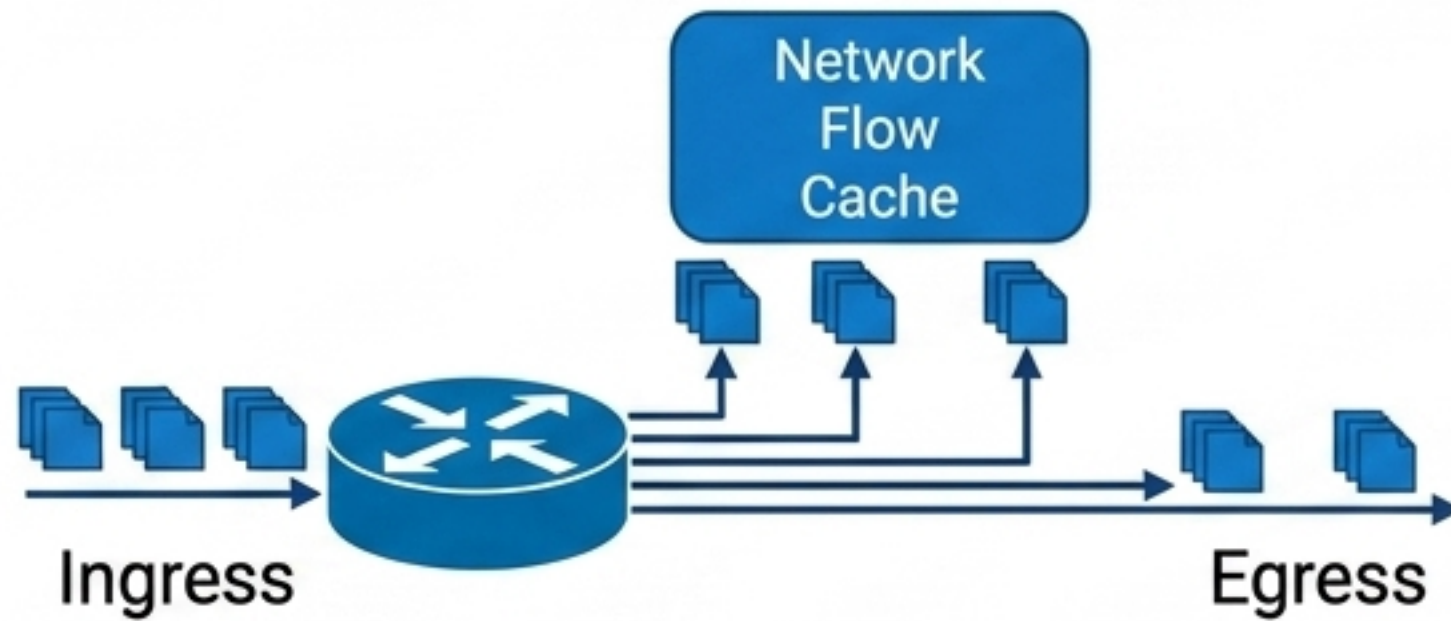
L'avantage majeur :

Détection sans signature. Les flux révèlent les comportements de reconnaissance inhabituels, éclairant les angles morts laissés par le chiffrement.



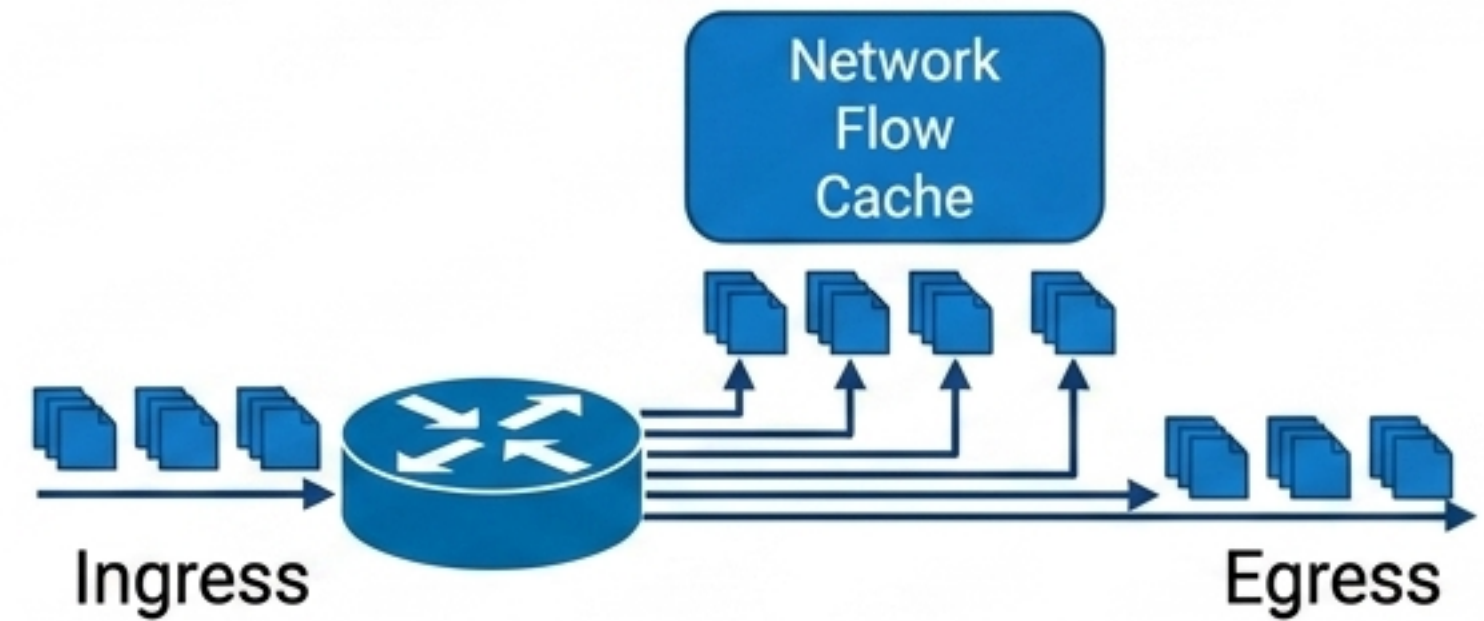
L'échantillonnage réseau introduit une détection probabiliste dangereuse pour l'investigation

Flux Échantillonné (Sampled)



- Examine 1 paquet sur N (ex: 1 sur 128).
- Économise le CPU, mais crée des trous dans la preuve forensique.

Flux Non Échantillonné (Unsampled)

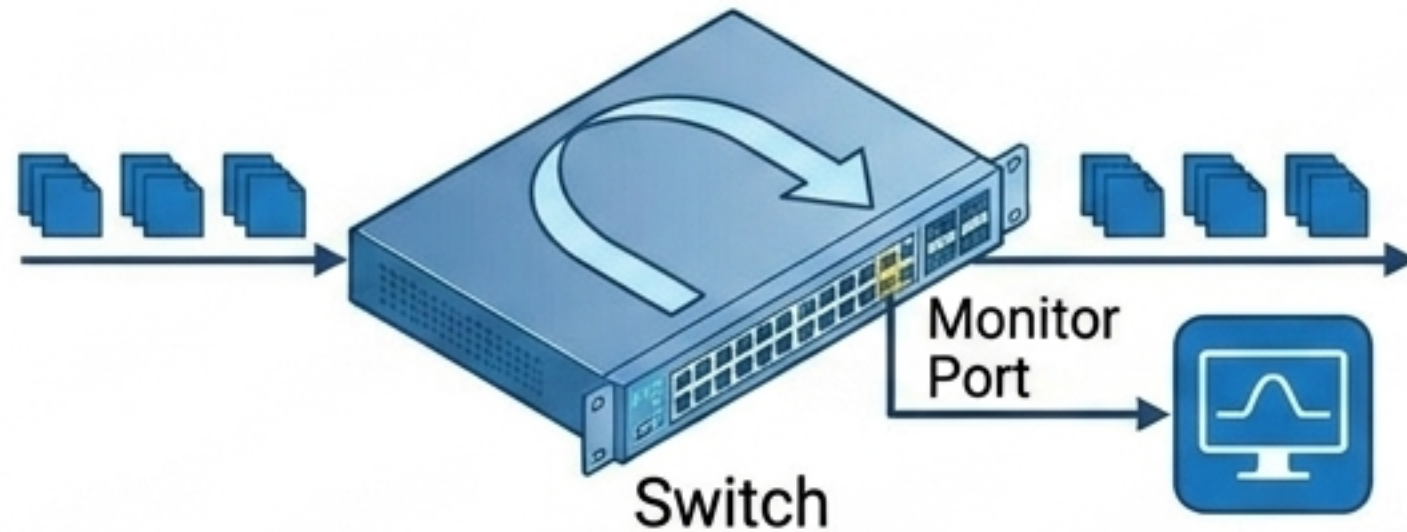


- Capture 100% du trafic.
- Exige plus de ressources, mais capture la vérité absolue.

Les flux échantillonnés vous disent que quelqu'un est entré chez vous hier.
Les flux non échantillonnés vous disent qu'il est actuellement dans votre salon.

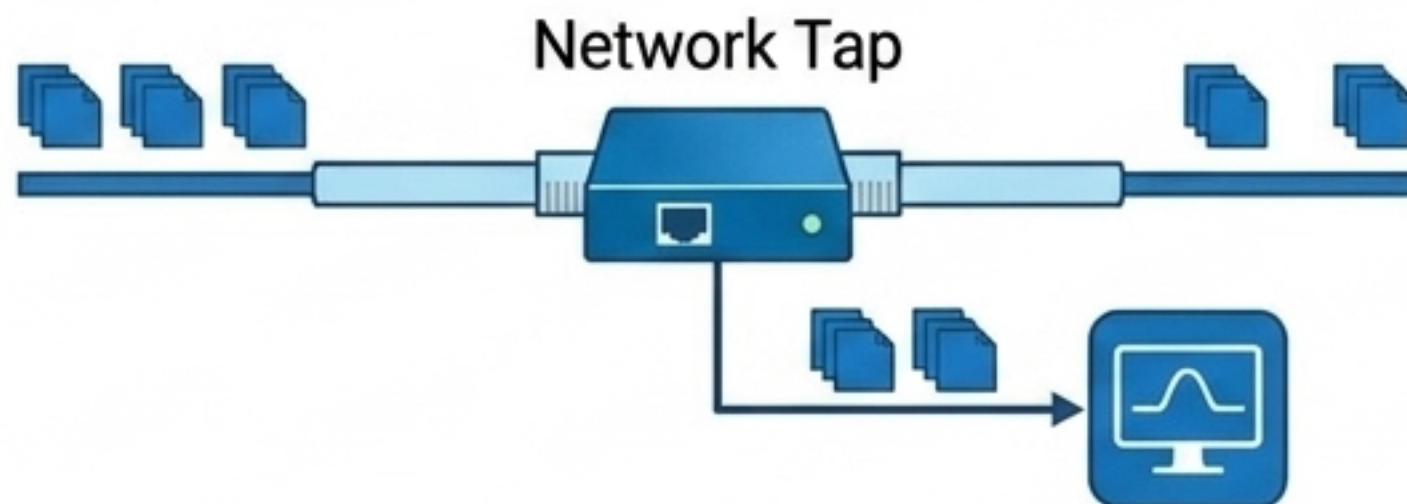
La capture de paquets bruts (PCAP) offre l'investigation la plus profonde

Mise en miroir (SPAN / RSPAN)



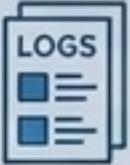
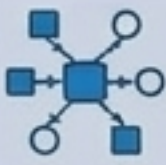
- Utilise les commutateurs existants pour dupliquer le trafic.
- Risque : Peut paralyser le commutateur s'il est surchargé (ex: miroir de 10 Gbit/s vers un port 1 Gbit/s).

Points d'écoute matériels (Network Taps)



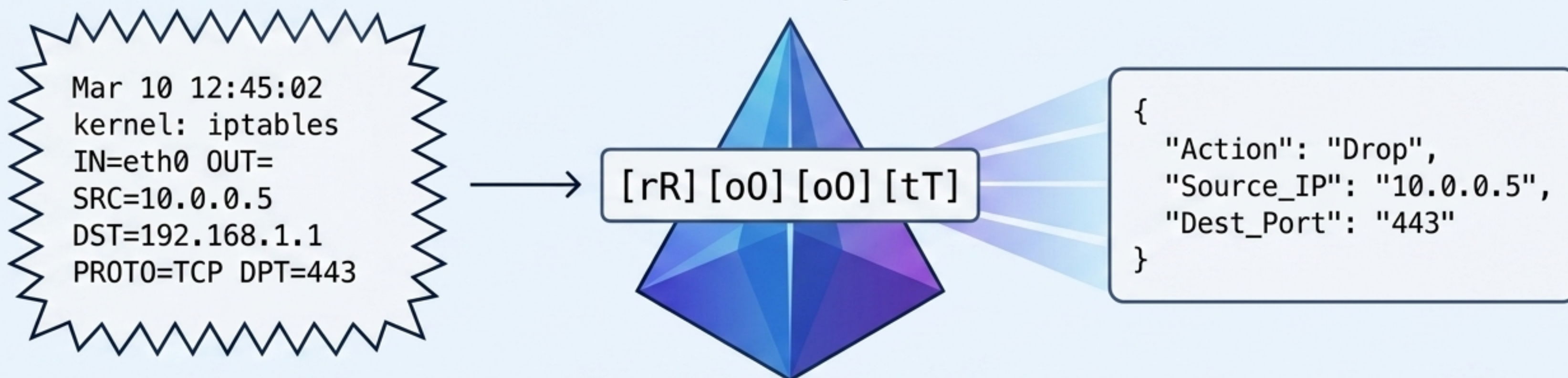
- Équipements passifs hors bande.
- Avantage : Zéro impact sur les performances du commutateur, capture garantie à 100%.
- Inconvénient : Déploiement coûteux ; limité aux centres de données critiques.

Matrice décisionnelle de télémétrie : Choisir la bonne profondeur technique

	Messages Journaux (Syslog)	Flux Réseau (NetFlow / IPFIX)	Capture de Paquets (PCAP)
Profondeur	 Faible à Moyenne (Événements système)	 Moyenne (Métadonnées de connexion)	 Maximale (Trafic brut complet)
Coût de stockage	 Faible à Moyen	 Moyen	 Extrêmement Élevé
Cas d'usage	Alertes de base, audit, conformité réglementaire   	Détection d'anomalies comportementales, cartographie   	Analyse forensique approfondie, inspection DPI   

Dompter le chaos : Analyse syntaxique (Parsing) et Expressions régulières

Moteur Regex



Sans un schéma de parsing connu par le SIEM, les données stockées restent un bloc de texte inexploitable.

Le cerveau du SIEM : Révéler les menaces grâce à la corrélation d'événements

La corrélation relie des événements disparates en utilisant le temps, les heuristiques et la valeur des actifs.

Force Brute

6 

Déclenché après 6 échecs d'authentification consécutifs.



Comportement Anormal

9

Déclenché lors de la création anormale de 9 nouveaux services ou processus.



Infections Massives

100 

Alerte réseau déclenchée si le seuil dépasse 100 hôtes infectés.



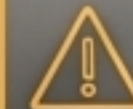
Malware Persistant

3 Jours 

Déclenché si l'hôte est incapable de nettoyer l'infection après 3 jours.



Sous le capot : Anatomie d'une règle de corrélation avec état



Attention : Les requêtes imbriquées complexes consomment énormément de ressources SIEM et peuvent générer des faux positifs.

L'intelligence avancée exige de comprendre ce qui est normal



Le Profilage Statistique (Baselining)

Établir l'EPS moyen, l'utilisation CPU/Mémoire, et les ports standards par jour de la semaine.



Détection d'anomalies

La sécurité ne dépend plus uniquement d'une règle pré-écrite. Le SIEM détecte les écarts massifs par rapport à la norme (ex: pics d'activité à plus de 3 écarts-types).



Conclusion : La combinaison d'une télémétrie rigoureuse (Journaux, Flux, PCAP) et d'une analyse comportementale forme la véritable fondation d'un SOC mature.