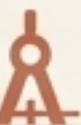




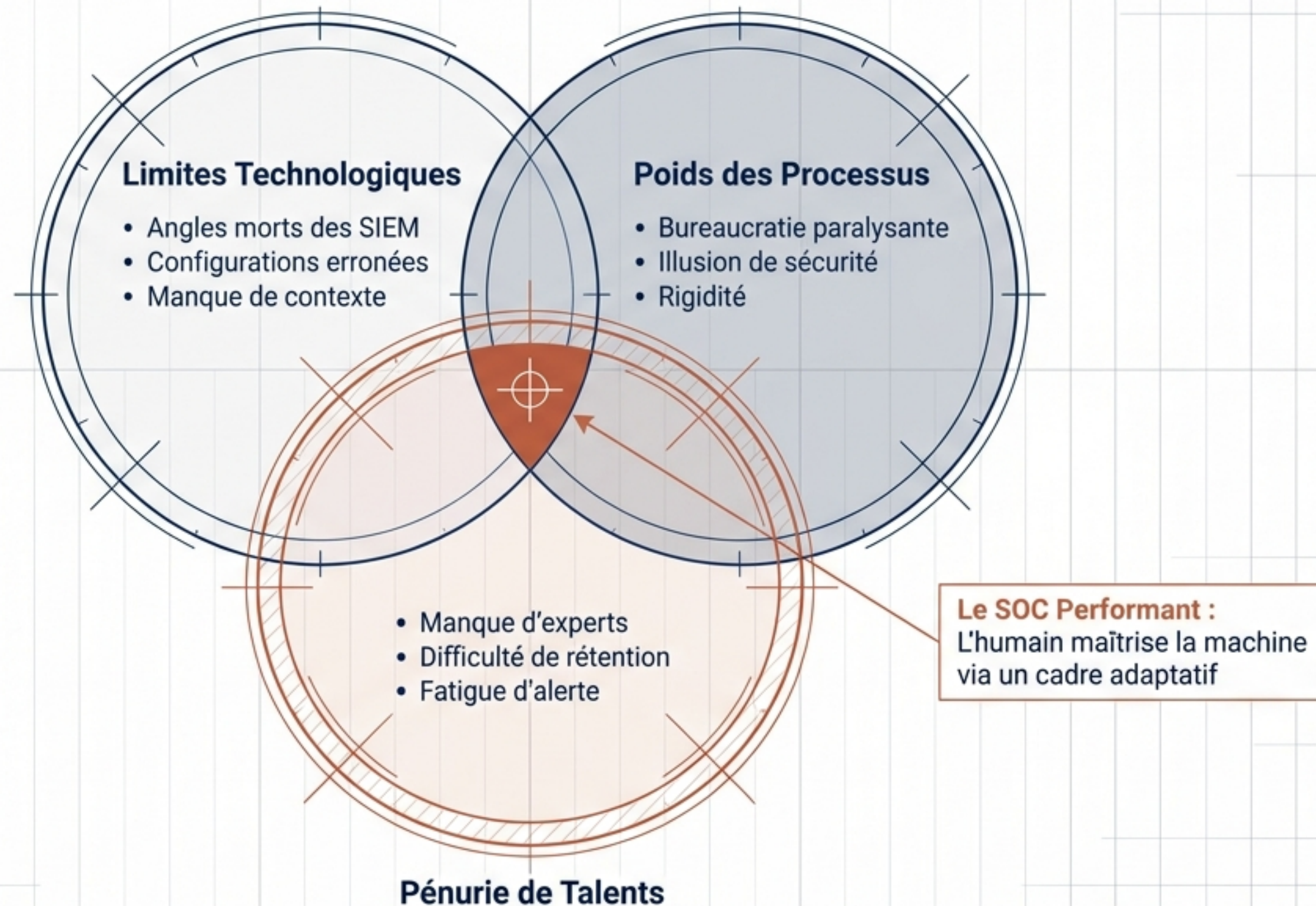
L'Humain au Cœur du SOC : Architecture, Talents et Processus

Un guide stratégique pour la conception et l'opérationnalisation
d'un centre de cyberdéfense performant.

« L'essentiel est de ne fréquenter que
des personnes qui vous élèvent, dont la
présence révèle le meilleur de
vous-même. » — Épictète

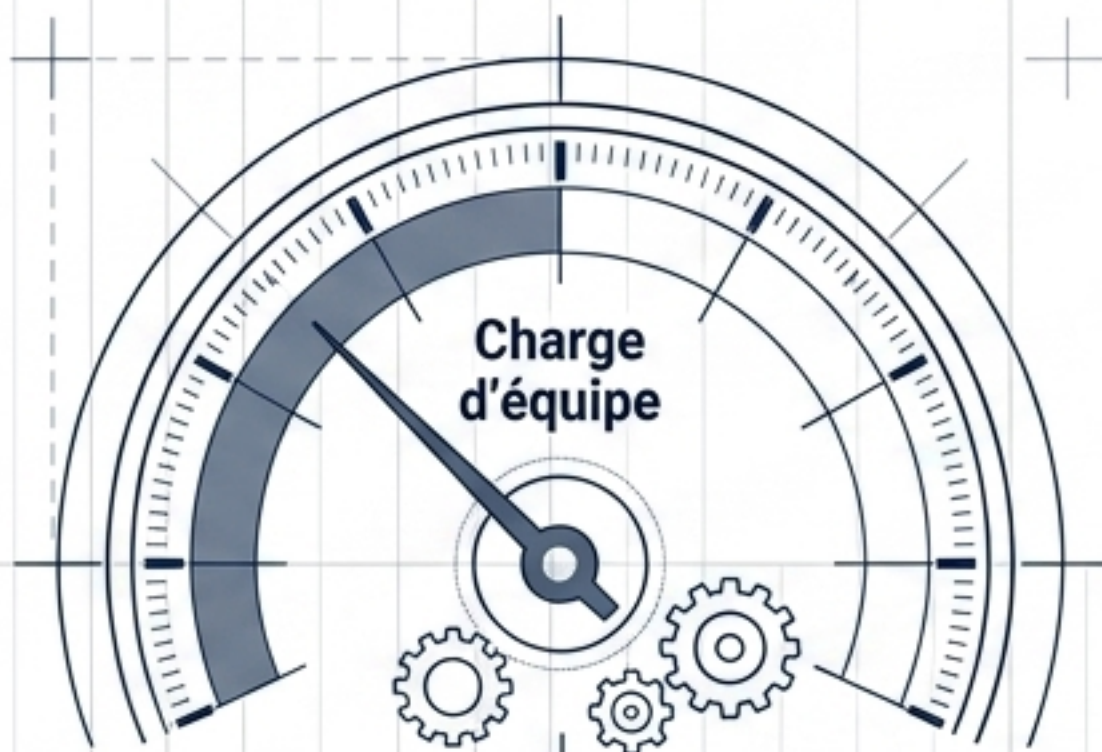


Le Mythe de la Technocratie : Les Défis Réels du SOC



Le Point de Départ Architectural : Définir la Mission

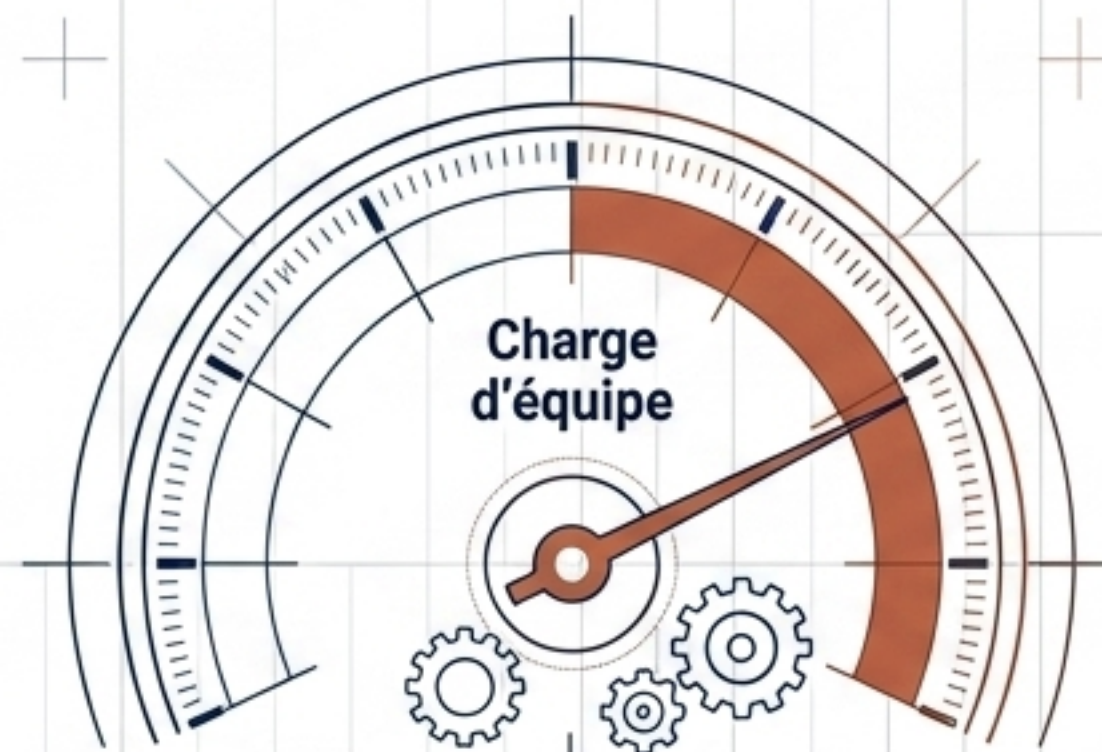
Le SOC « Classique »



- Surveillance en temps réel
- Triage et réponse initiale (Niveau 1)
- Détection de base

Frontière : Remédiation et ingénierie externalisées.

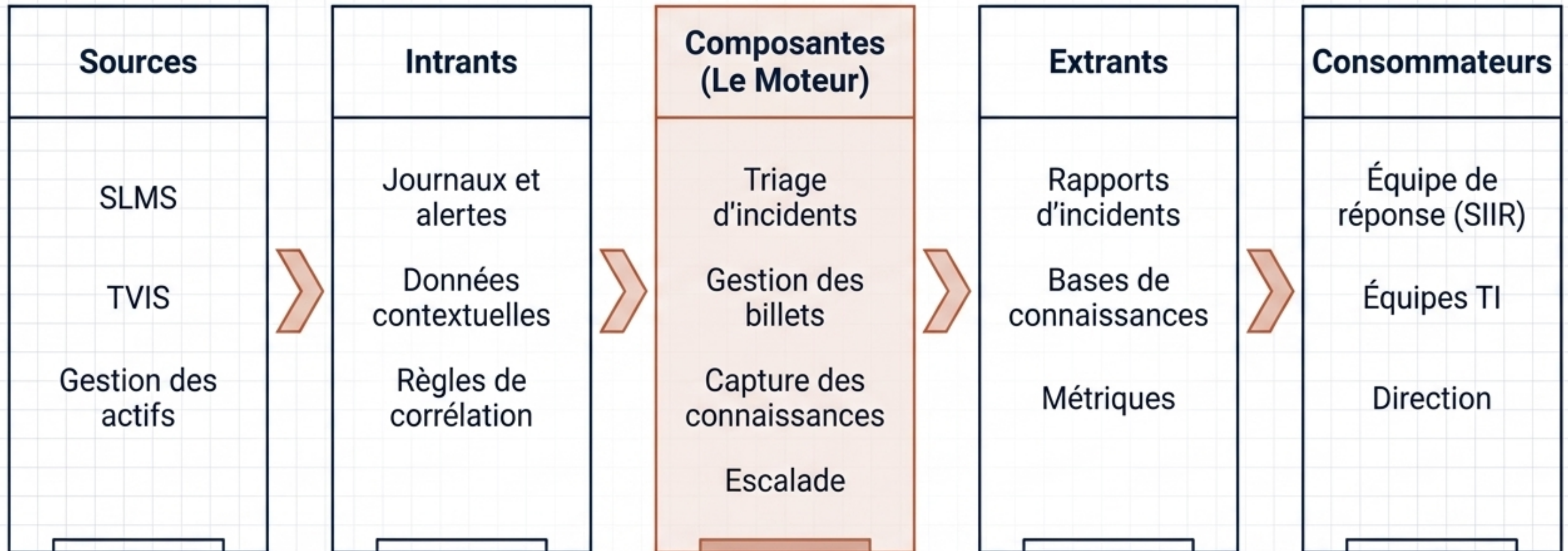
Le SOC « Étendu »



- Renseignement sur les menaces (TVIS)
- Ingénierie des plateformes de sécurité
- Gestion des clés et données cryptographiques
- Analyse post-violation (Forensic)

Conséquence : Nécessite des sous-équipes spécialisées sous direction commune.

Anatomie Structurale d'un Service : La Surveillance de Sécurité



Paramètres Directeurs : Couverture 24/7 | Contraintes financières | SLAs de temps de réponse

Cartographie Modulaire des Services SOC

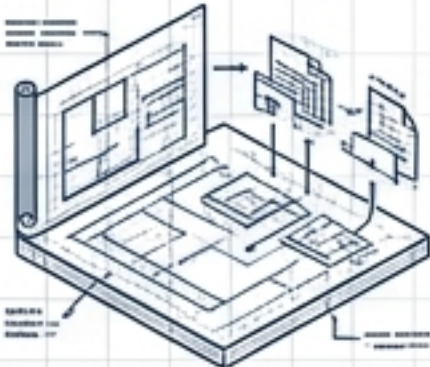
Pilier 1 : Gouvernance (SSM)



- Alignement ITIL
- Audits et conformité
- Optimisation des coûts

Pilier 2 : Construction & Maintenance

Ingénierie (SSE) :
Conception des plateformes

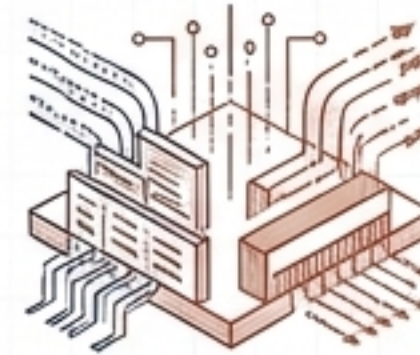


Opérations (SSO) :
Stabilité et changements

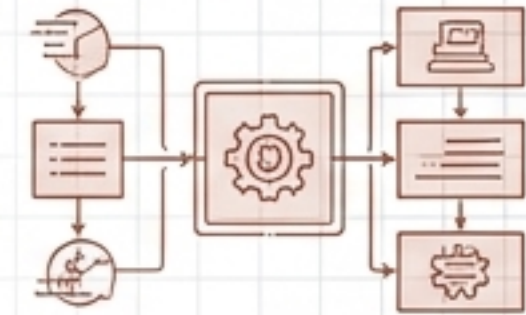


Pilier 3 : Détection & Enquête

Journaux (SLMS) :
Collecte de données



Réponse (SIIR) :
Validation et remédiation

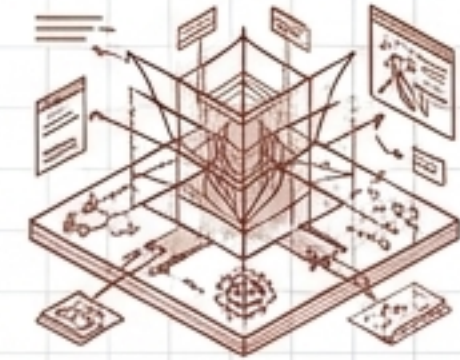


Pilier 4 : Intelligence

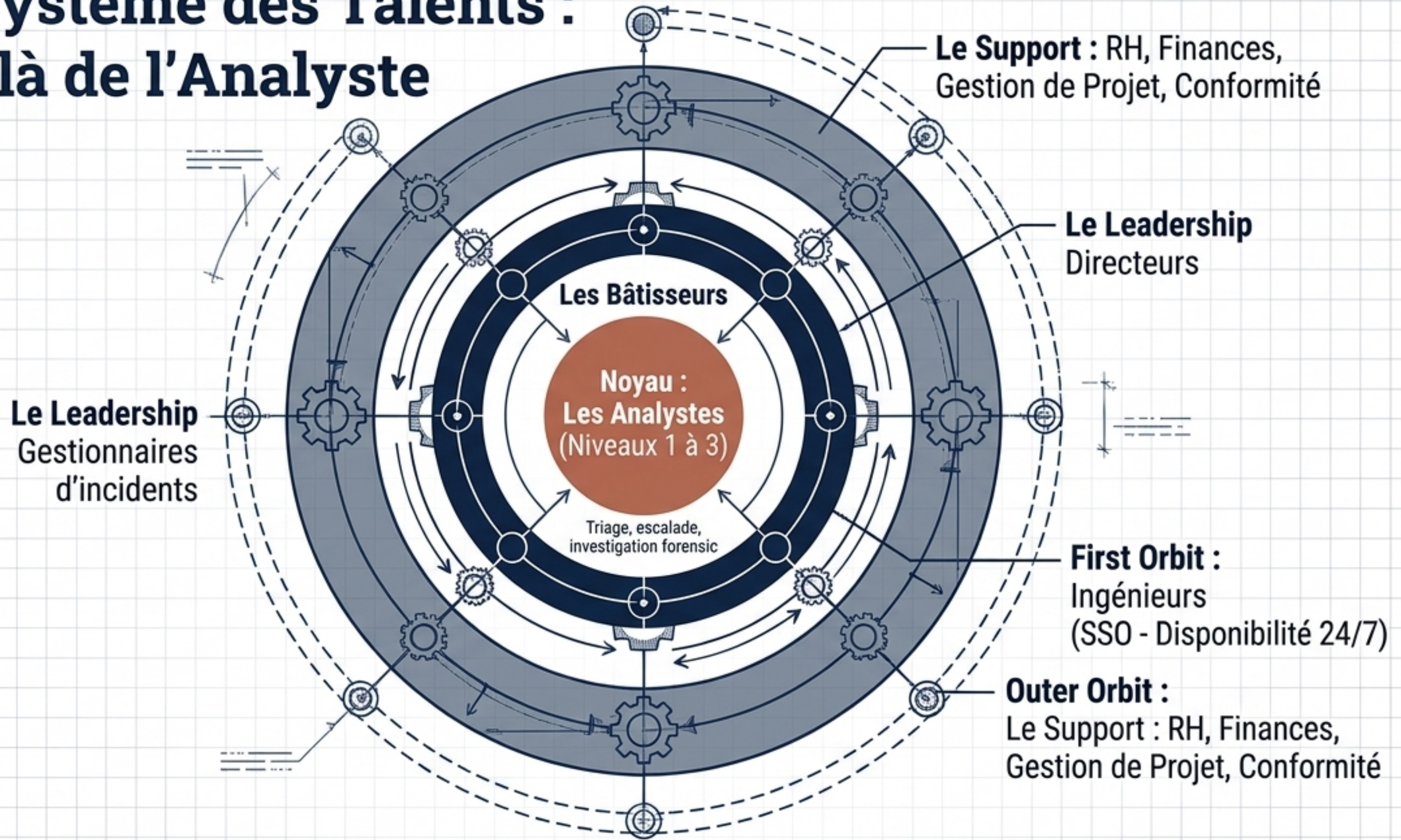
Vulnérabilités (VDS) :
Découverte des failles



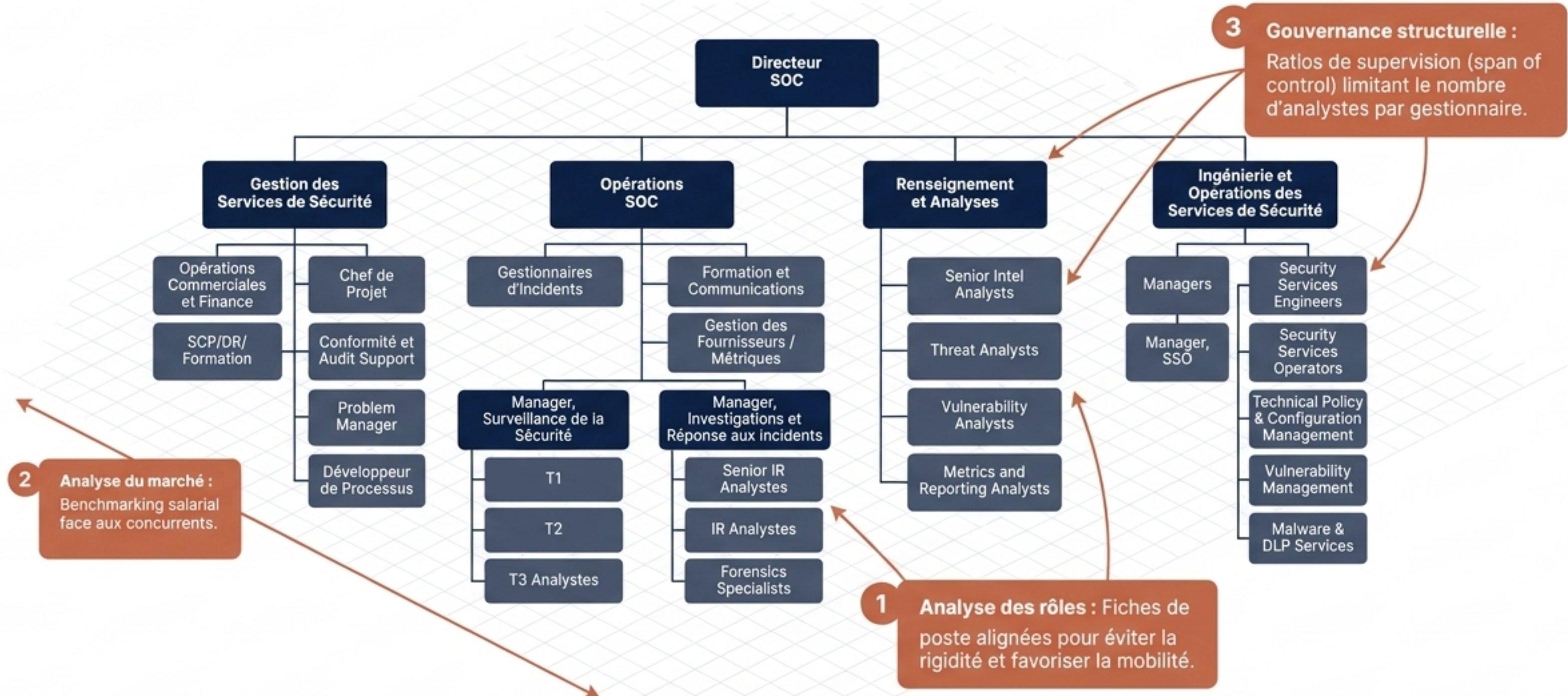
Menaces (TVIS) :
Modélisation émergente



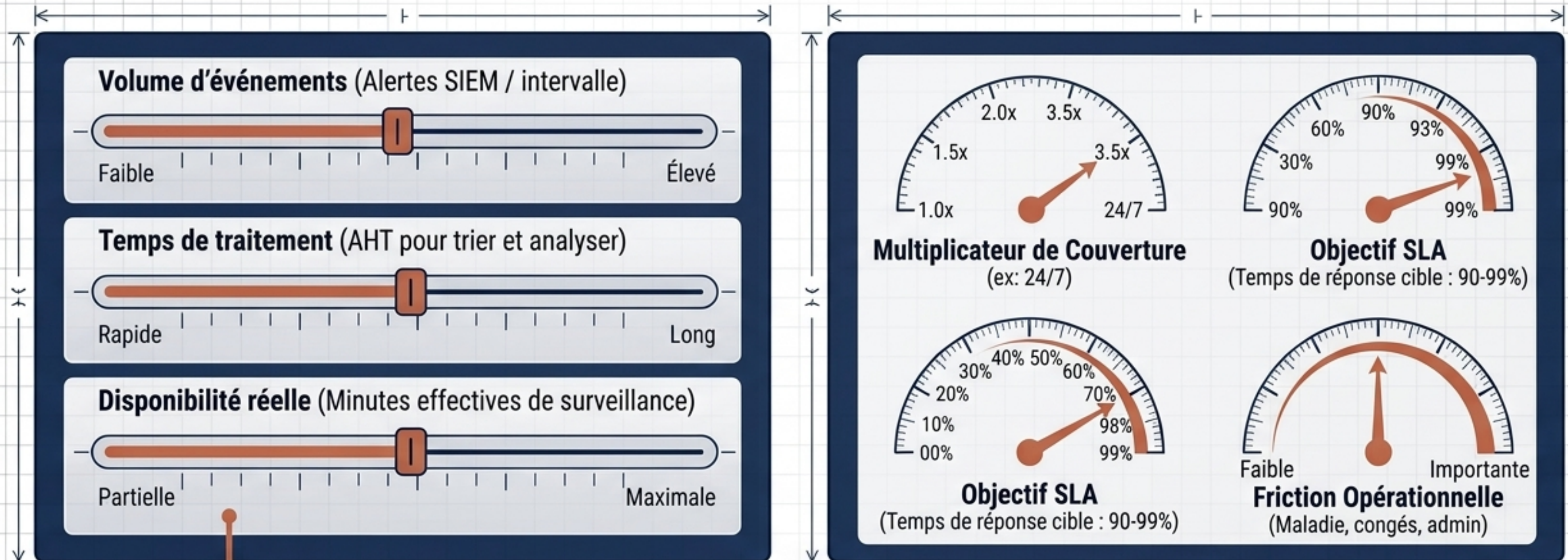
L'Écosystème des Talents : Au-delà de l'Analyste



L'Ingénierie Organisationnelle (Le rôle clé des RH)



La Mathématique de la Capacité : Calculer l'Effectif



L'équation est théorique : seul le premier incident majeur validera la taille réelle de l'équipe.

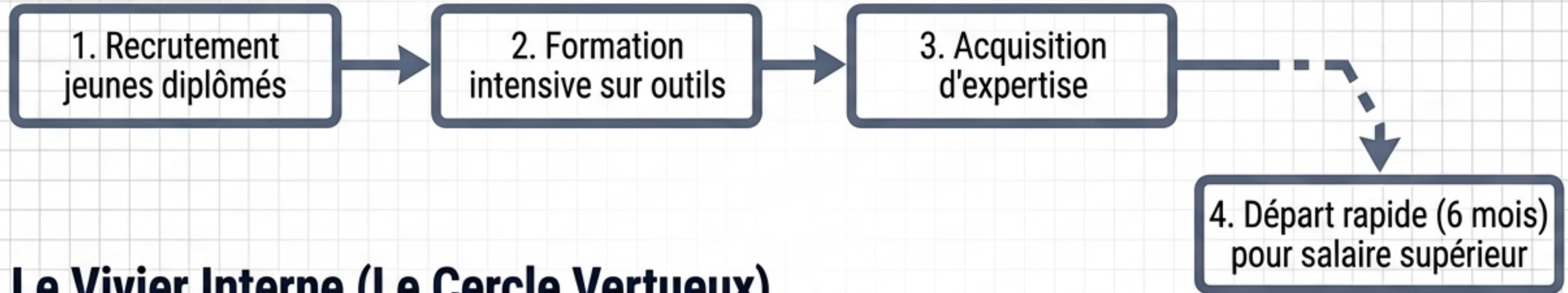
Modèles d'Approvisionnement : La Matrice Décisionnelle

	Interne (Équipe propre)	Consultants (Contrats)	Impartition (Externalisation)	Services Gérés (MSSP)
Vitesse de déploiement	 Variable	 Optimal	 Optimal	 Optimal
Connaissance du contexte d'entreprise	 Optimal	 Variable	 Variable	 Suboptimal
Capacité de rétention des savoirs	 Optimal	 Suboptimal	 Variable	 Variable
Tâches à haut volume (Niveau 1)	 Variable	 Optimal	 Optimal	 Optimal
Accès à l'expertise de niche (Forensic)	 Suboptimal	 Variable	 Optimal	 Optimal

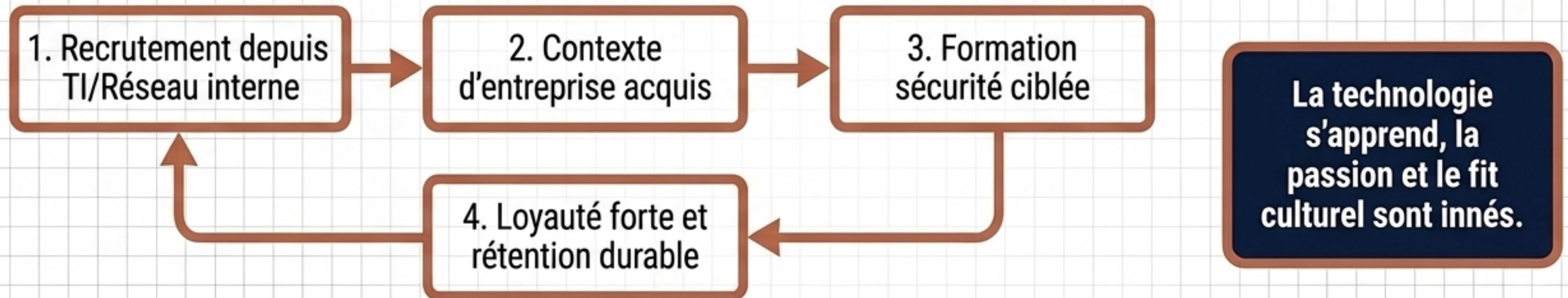
 Optimal |  Variable |  Non recommandé

Le Paradoxe de la Rétention : Éviter le Seau Percé

Le Piège des Diplômés (Le Seau Percé)

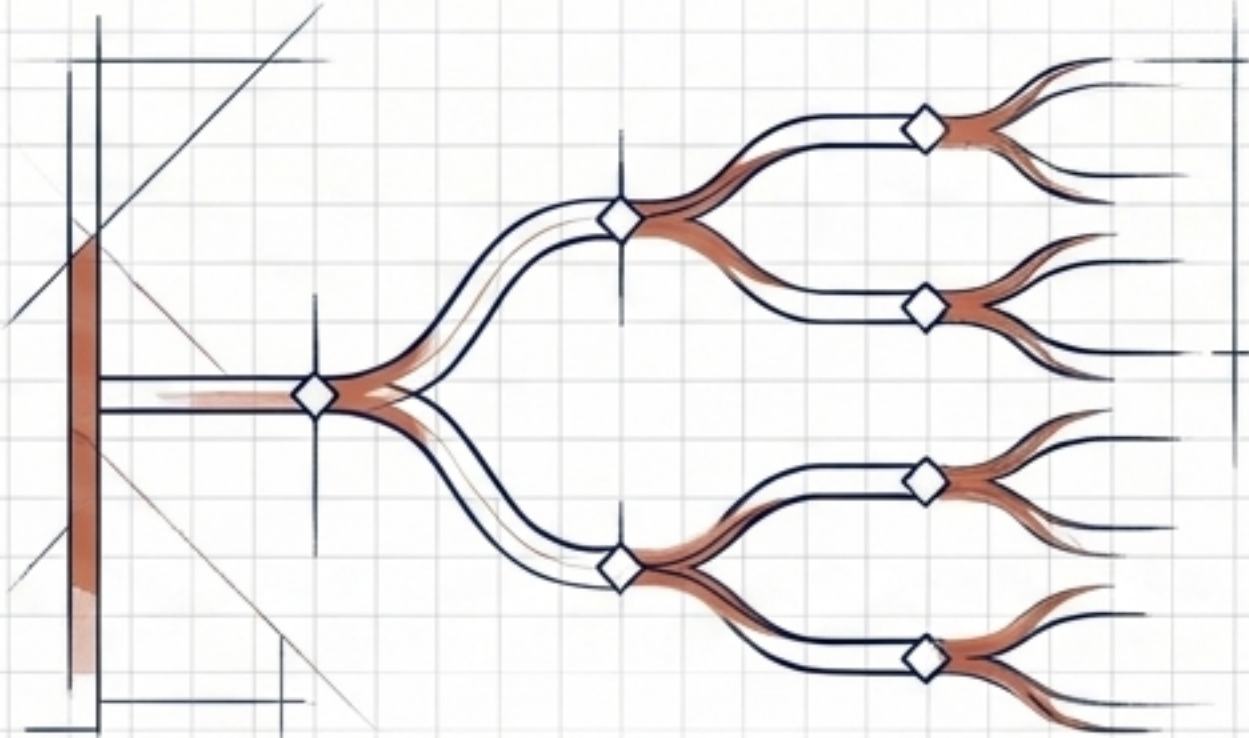


Le Vivier Interne (Le Cercle Vertueux)



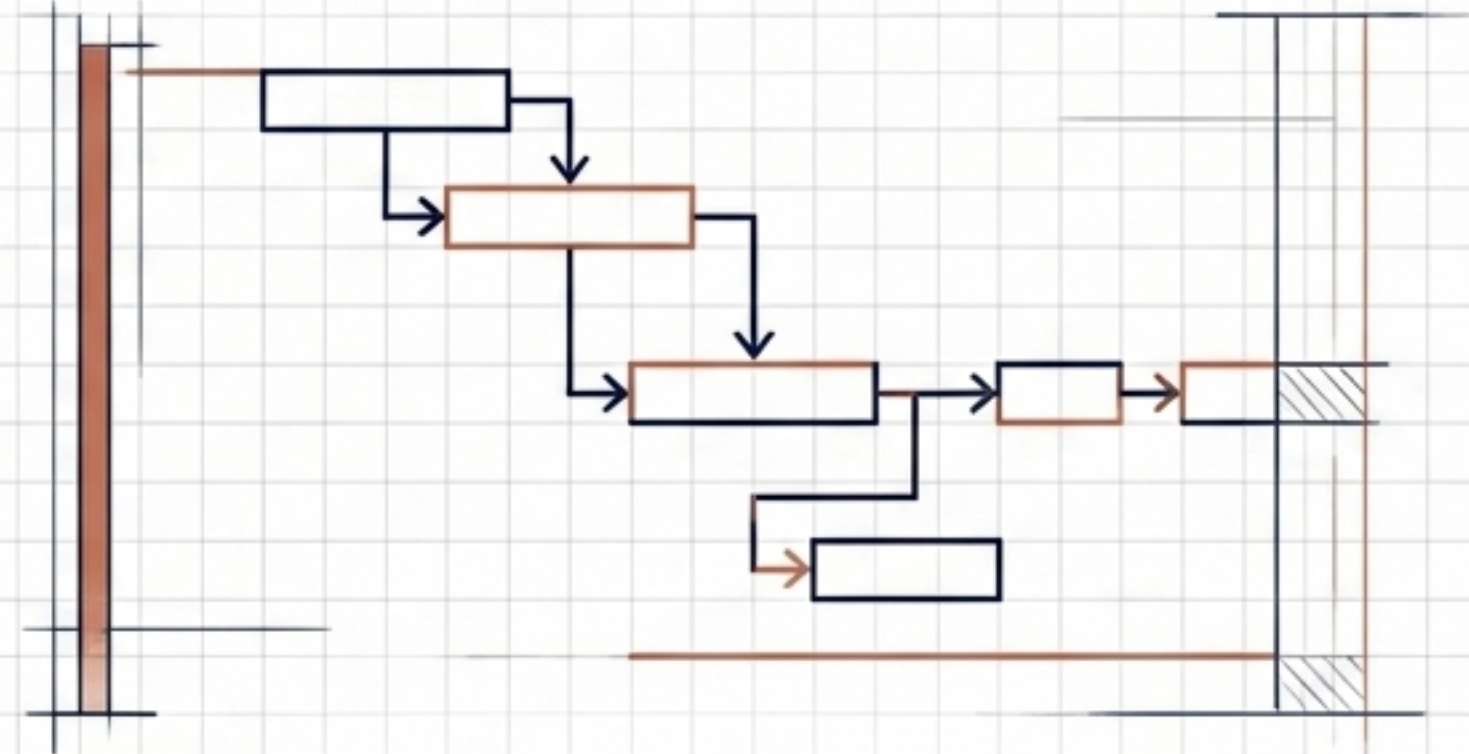
Le Grand Débat : Processus vs Procédure

Processus (Le Cadre Agile)



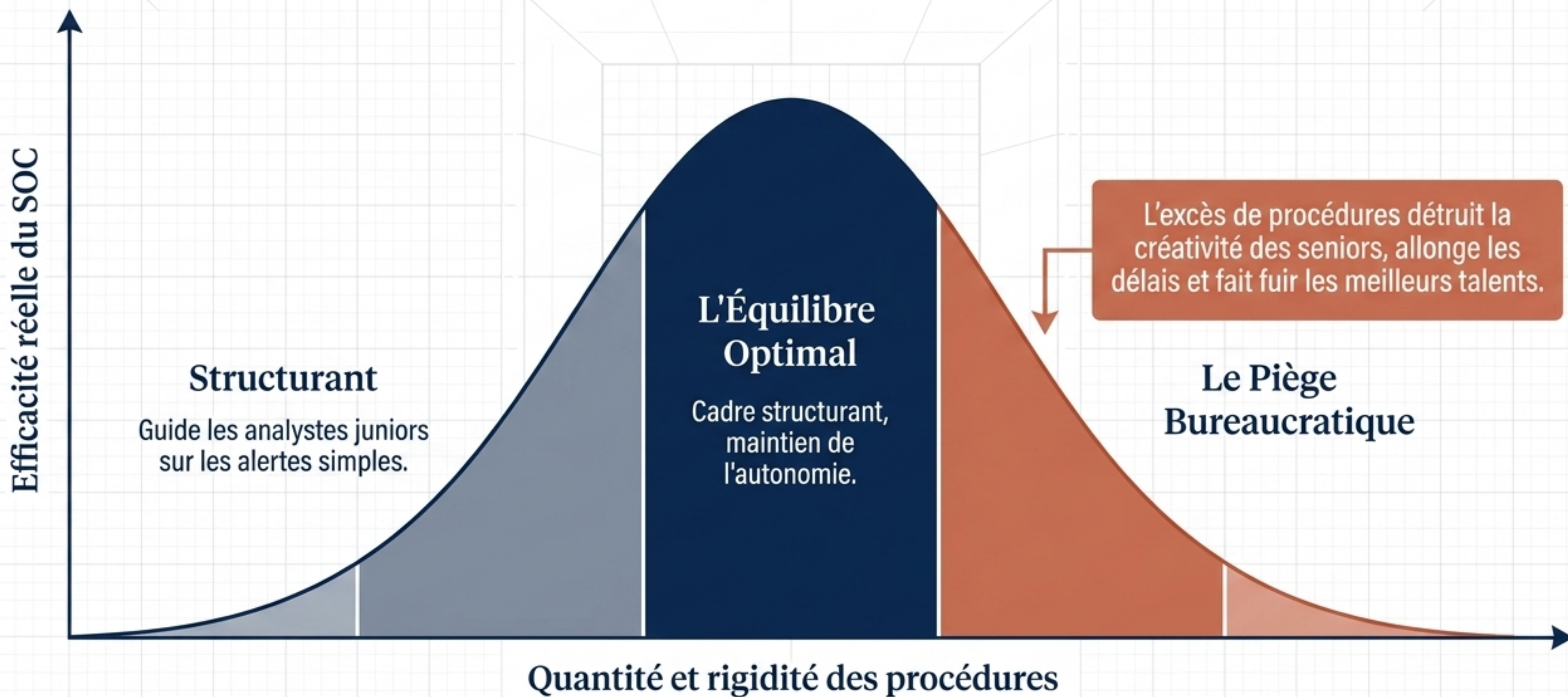
- **Définition** : Actions partagées pour un objectif commun.
- **Caractéristiques** : Évolutif, options multiples, collaboratif.
- **Application SOC** : Gestion d'une investigation complexe.

Procédure (Le Manuel d'Exécution)

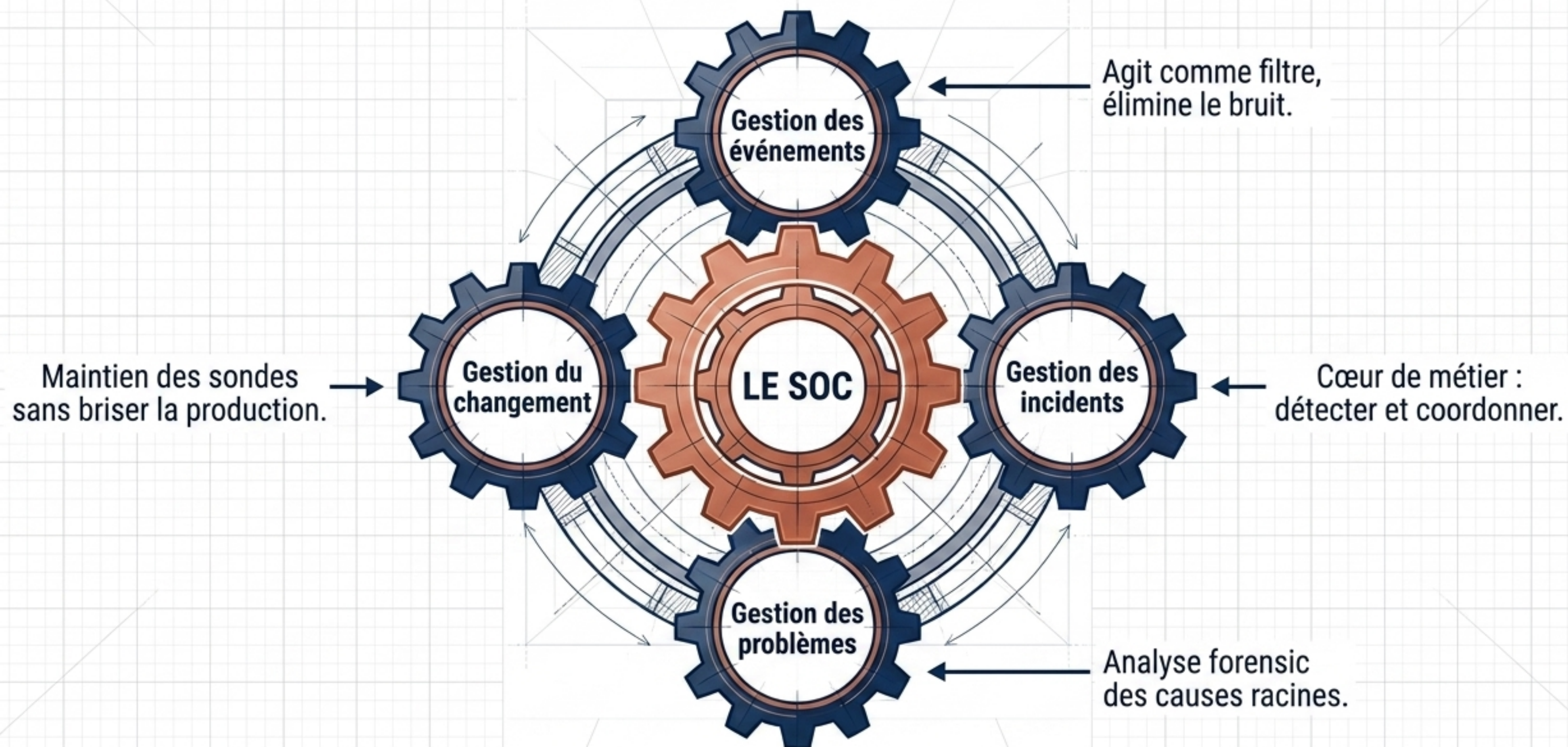


- **Définition** : Méthode prescrite étape par étape, sans déviation.
- **Caractéristiques** : Binaire (suivi ou non), aucune option, rigide.
- **Application SOC** : Ouverture standardisée d'un billet TI.

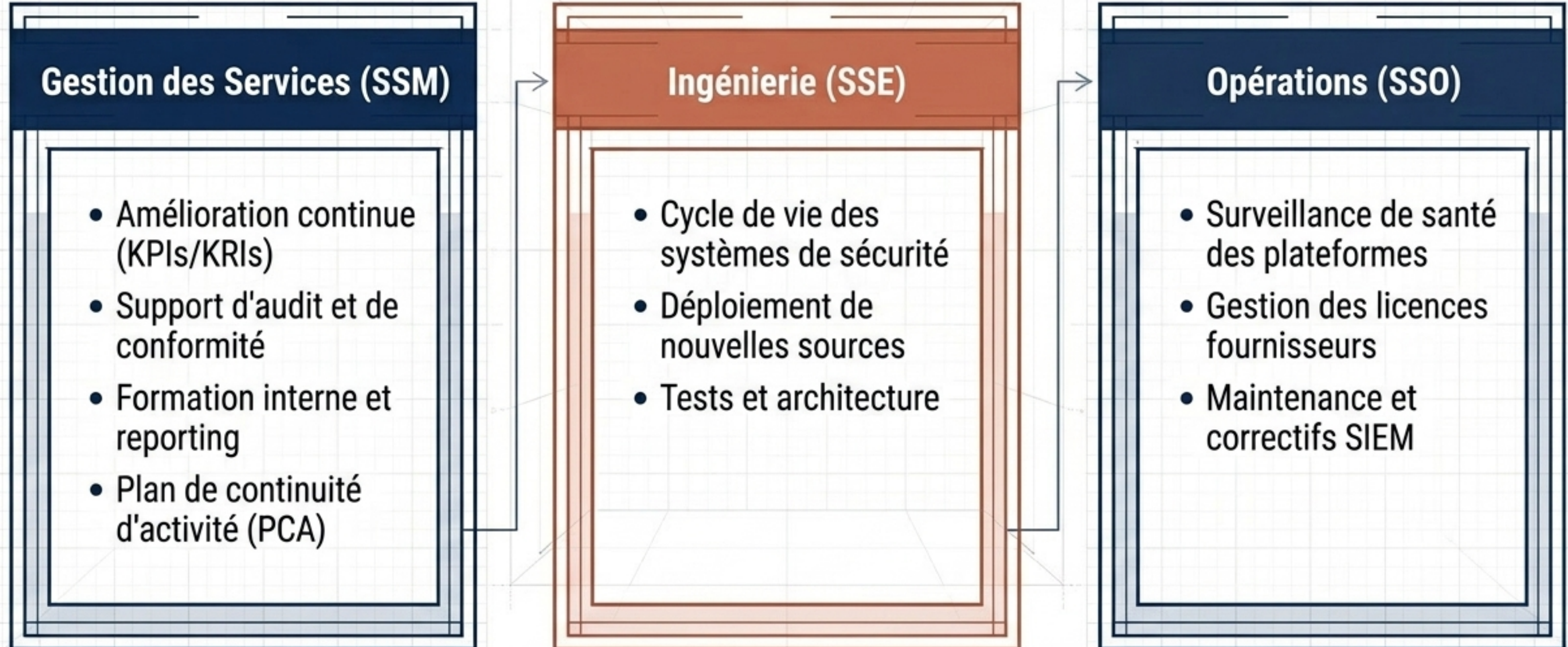
Le Paradoxe de la Bureaucratie : Le Poids des Processus



L'Intégration ESM : Brancher le SOC sur l'Entreprise



Le Portefeuille des Processus Vitaux du SOC



Synthèse : Le SOC comme Organisme Adaptatif



L'excellence d'un SOC ne réside pas dans l'empilement de ses outils, mais dans la capacité de son talent humain à interpréter l'inconnu grâce à un cadre qui encourage l'expertise créative.