Chapitre 1.1 — Comprendre les concepts clés en Incident Management, Monitoring et Observabilité

Objectif du chapitre

Avant d'agir efficacement face à un incident, **il faut bien comprendre ce que l'on vit**.Ce premier chapitre est là pour construire **votre socle de compréhension** et vous donner des **réflexes solides**.

À la fin de ce chapitre, vous saurez :1) Nommer précisément ce que vous vivez (incident, problème, crise, catastrophe)
2) Piloter vos actions avec les bons indicateurs (RTO, RPO, SLA...)

3) Comprendre ce qu'est **l'observabilité** et pourquoi elle change tout

4) Vous repérer dans les **grands standards de la gestion des incidents**

1.1.1 Incident, Problème, Crise, Catastrophe : apprendre à bien qualifier

Pourquoi c'est essentiel ?

> "Ce qu'on nomme mal, on le combat mal." (inspiré de Camus)

Avant de résoudre, **il faut qualifier** :

- Est-ce un souci localisé ?
- Est-ce une faille systémique ?
- Faut-il mobiliser une cellule de crise ?
- Faut-il activer un plan de continuité ?

Comment qualifier l'incident ?

Problème localisé

Nécessite une attention immédiate mais n'escalade pas davantage.

Faille systémique

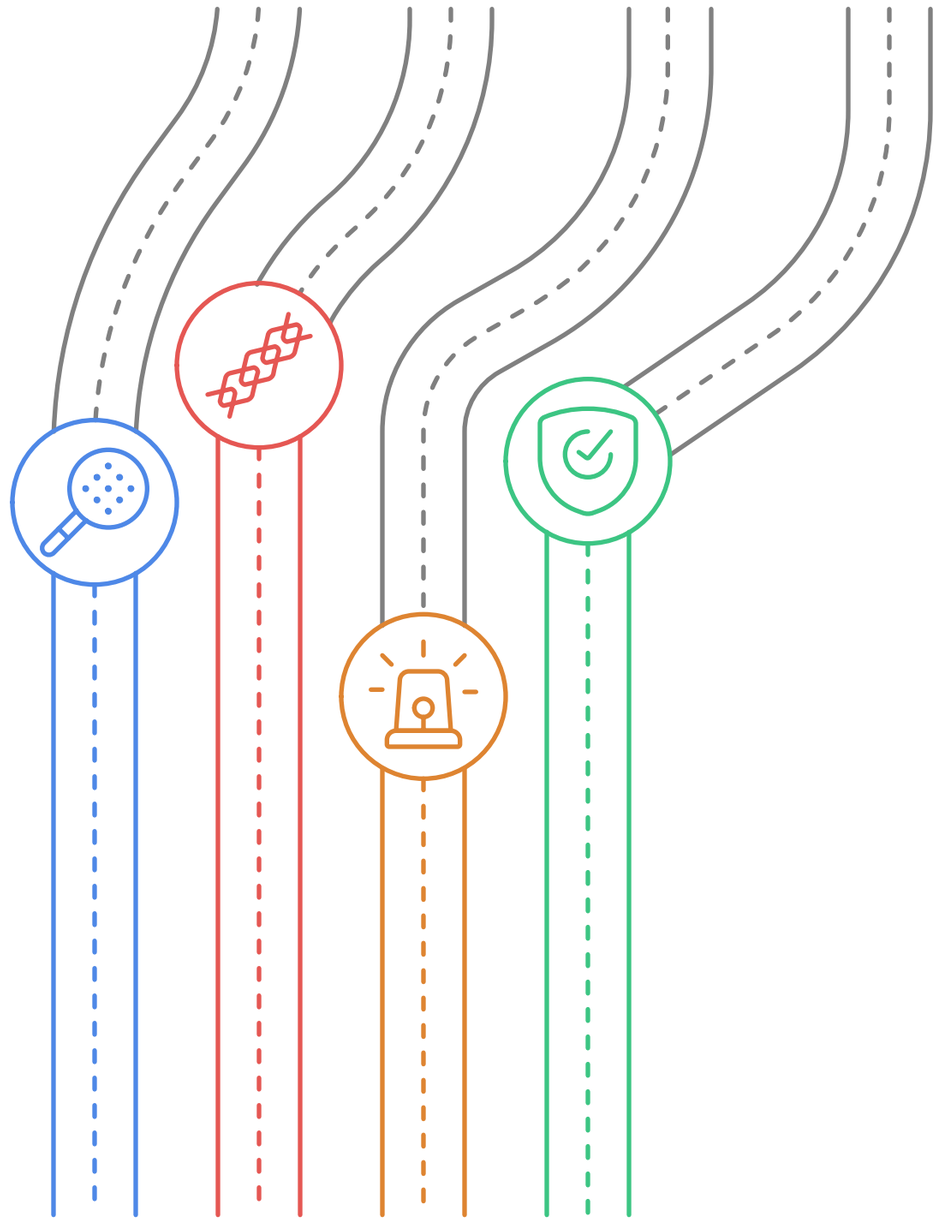
Nécessite une analyse et une correction à l'échelle du système.

Mobiliser une cellule de crise

Nécessite une réponse coordonnée à grande échelle.

Activer un plan de continuité

Nécessite des mesures pour maintenir les opérations.



Lexique simplifié avec analogies

Hiérarchie des événements de gestion des incidents

Incident

Dysfonctionnement isolé et limité

Problème

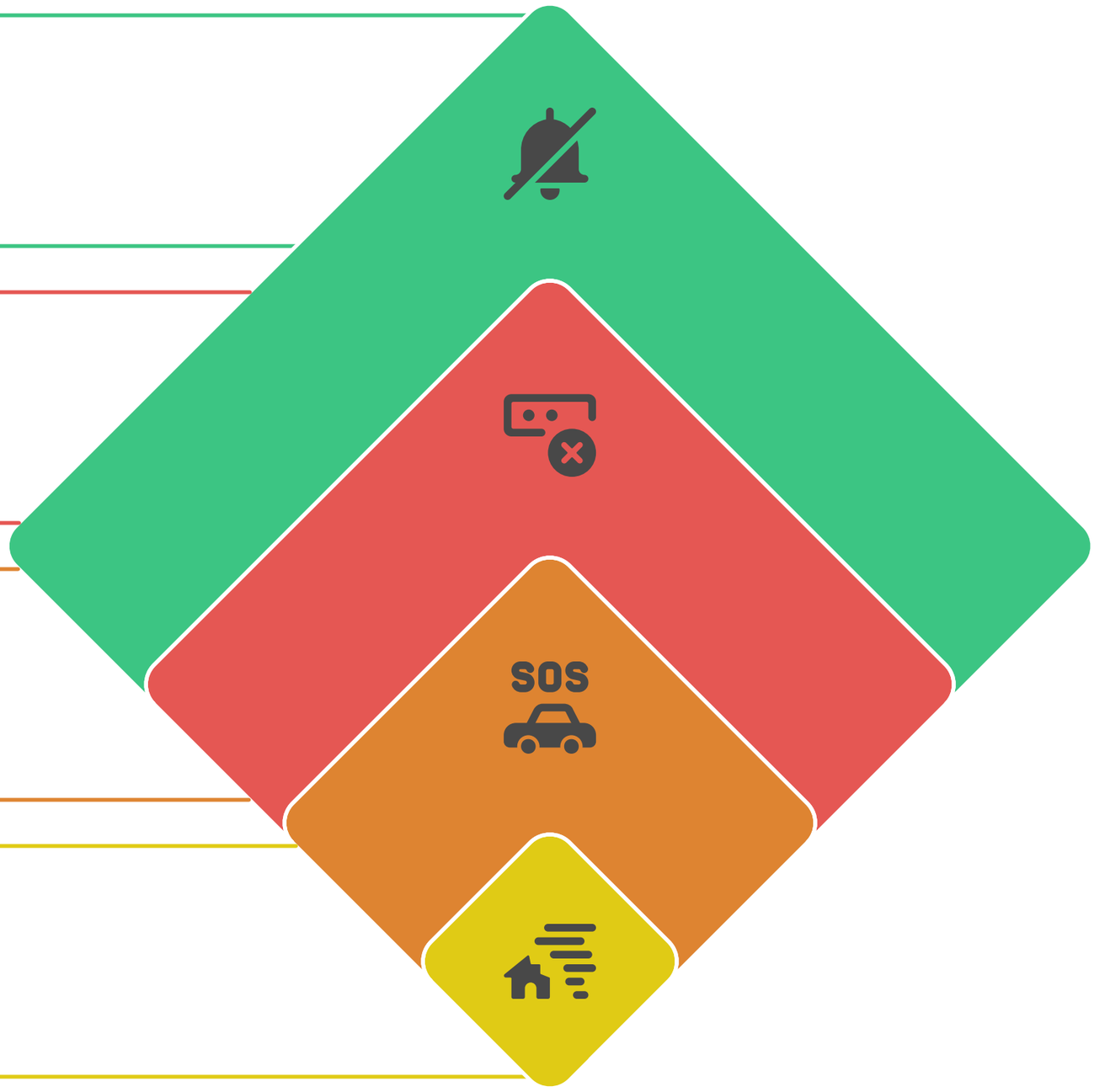
Cause fondamentale d'incidents répétés ou graves

Crise

Événement majeur nécessitant une mobilisation d'urgence

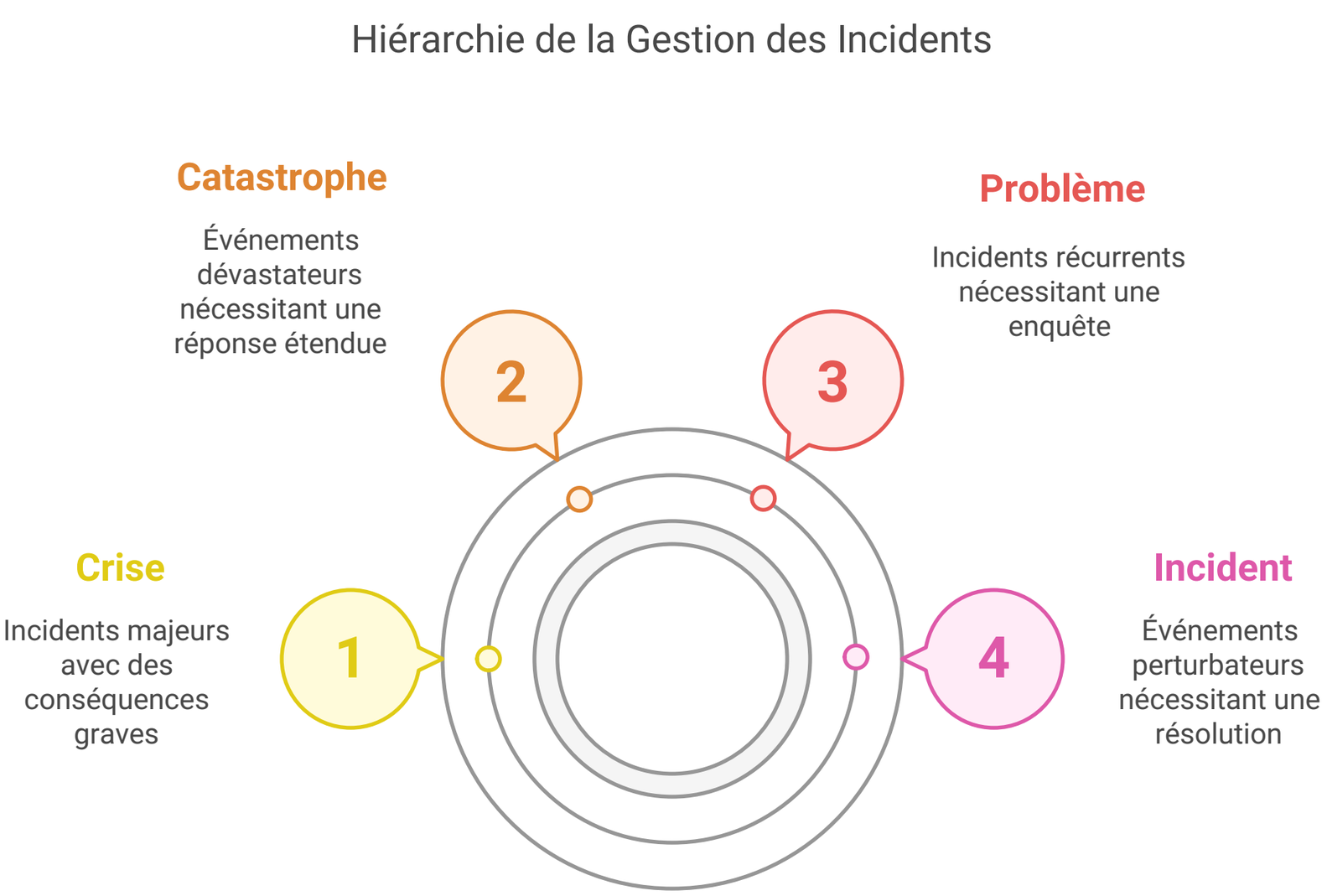
Catastrophe

Événement extrême compromettant l'activité à long terme



Synthèse simple

> ☒ "Pas tout est une crise. Tout n'est pas un incident léger.
>
> ☒ Bien nommer = Bien gérer."



Conseil pratique pour le terrain

- Toujours **analyser l'impact métier** : ☒ Combien de clients impactés ?
- ☒ Quel risque réputationnel ?

- ☒ Combien de perte financière par heure ?

Analyse d'Impact Métier

Problème de Réputation

Problème de réputation malgré un faible impact client.

Crise Majeure

Crise majeure avec impact client et risque réputationnel élevé.

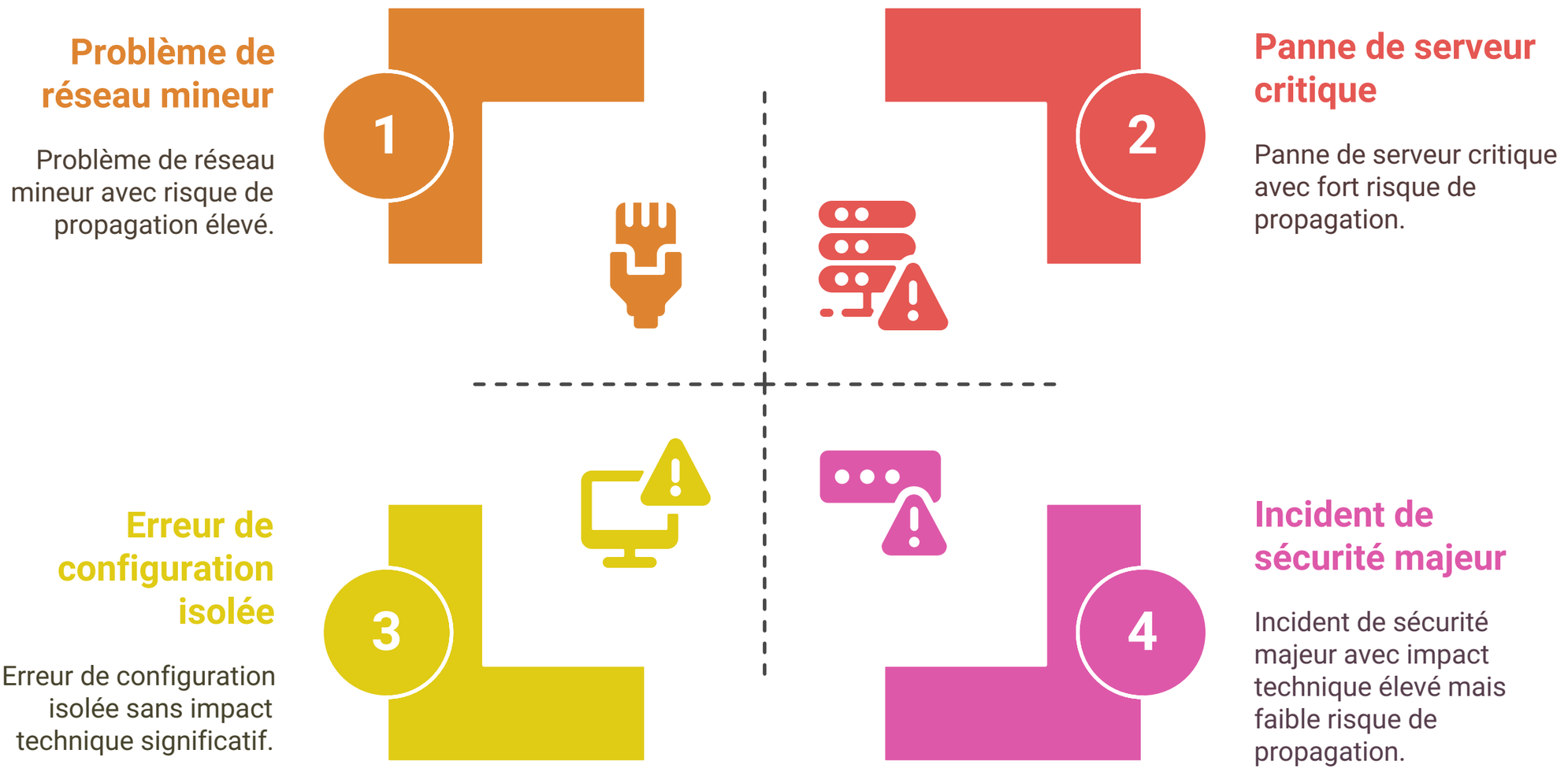
Incident Mineur

Incident mineur avec faible impact client et risque réputationnel.

Impact Client Significatif

Impact client significatif mais faible risque réputationnel.

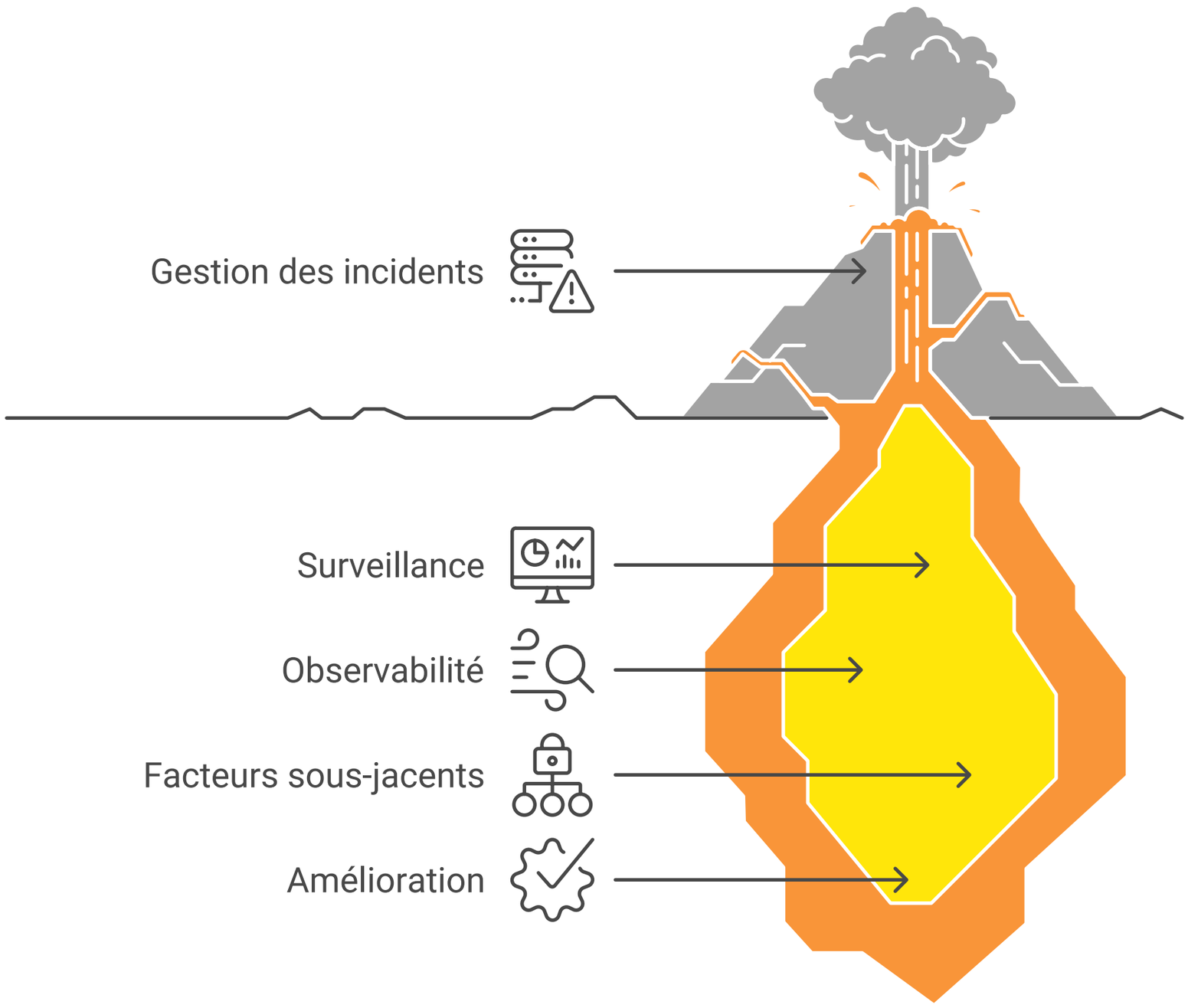
- Toujours **analyser l'impact IT** : Combien de serveurs/services affectés ?
- Quel périmètre technique ? Quel risque de propagation ?



1.1.2 Les indicateurs critiques : RTO, RPO, SLA, SLO, SLI

Pourquoi c'est essentiel ?

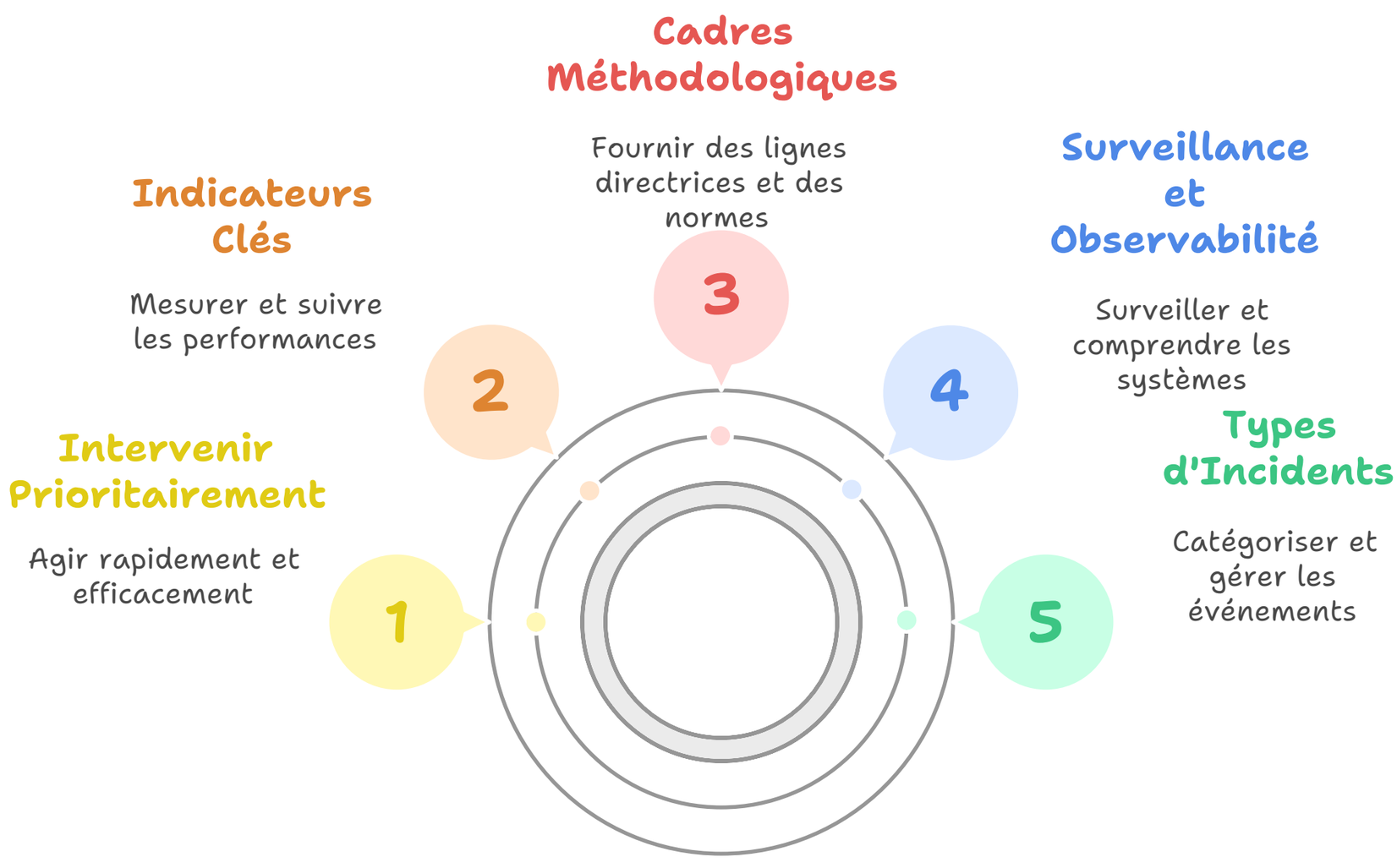
> "Ce qu’on ne mesure pas, on ne peut pas améliorer."



En gestion d’incident, vous êtes comme un pompier :

- **Vous devez savoir où intervenir en priorité**

Hiérarchie de la Gestion des Incidents



- **Combien de temps vous avez pour sauver ce qui peut l’être**

Comment gérer efficacement les incidents pour minimiser les pertes ?

Récupération rapide

Minimise les pertes et les temps d'arrêt

VS

Récupération lente

Augmente les pertes et les temps d'arrêt

Définitions claires + métaphores

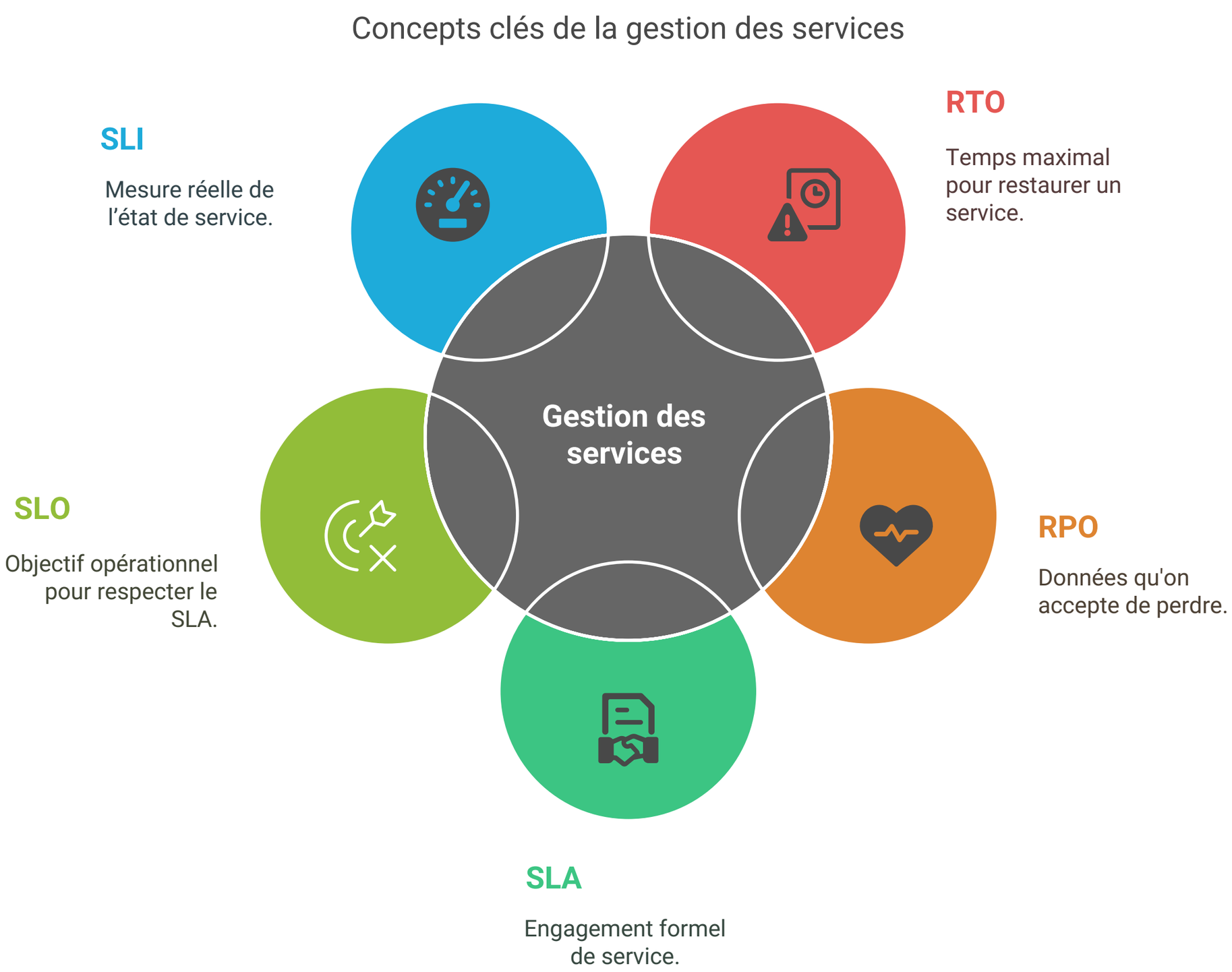
RTO Temps maximal pour restaurer un service (exemple:Durée de survie sans oxygène.)

RPODonnées qu'on accepte de perdre.(exemple: Minutes acceptables sans battement cardiaque en réanimation)

SLAEngagement formel de service.(exemple: Contrat de livraison garantie)

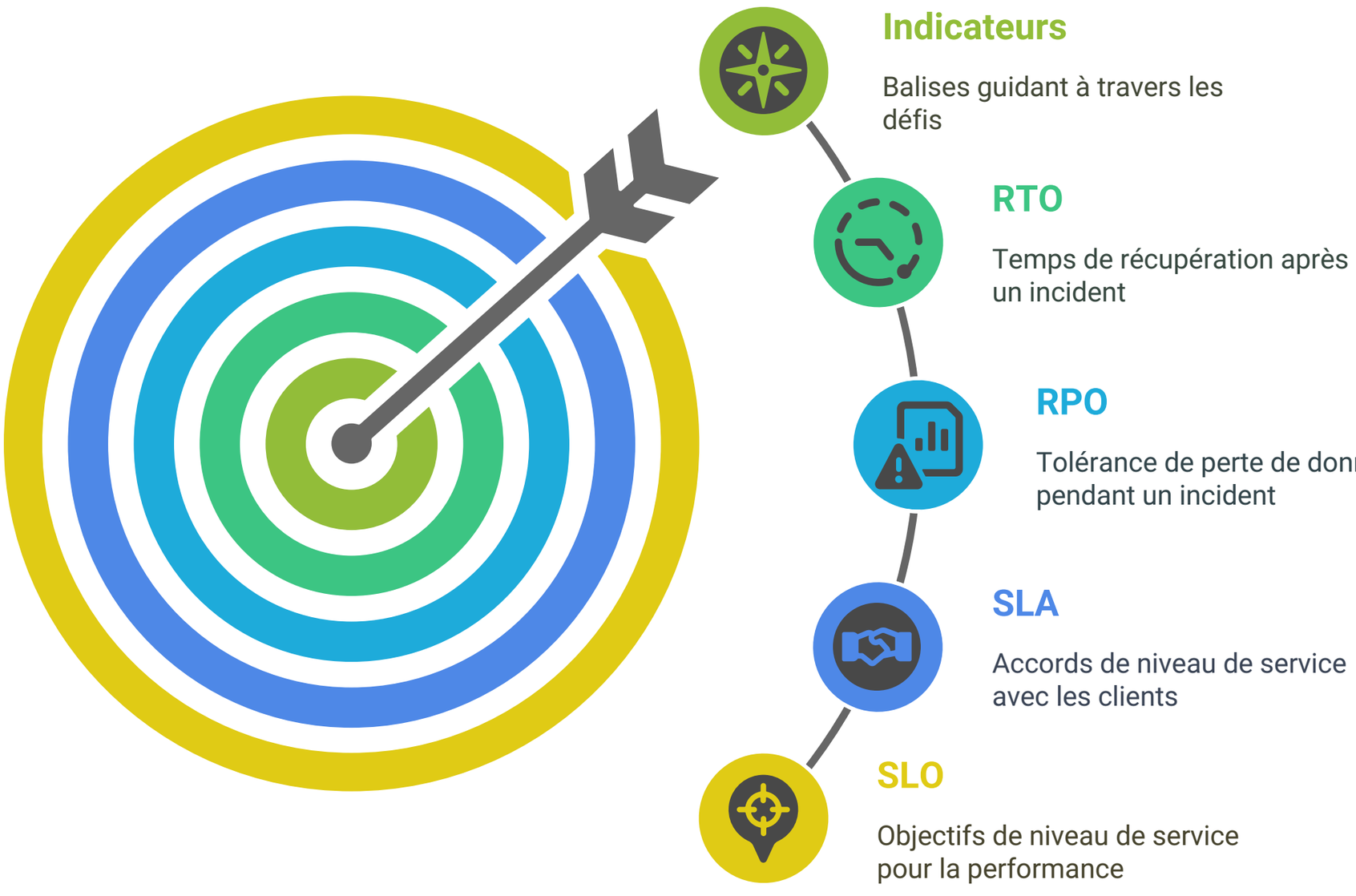
SLOObjectif opérationnel pour respecter le SLA.(exemple: Viser la livraison 10 minutes avant la limite pour être sûr)

SLIMesure réelle de l’état de service (exemple: Chronomètre dans la course contre la montre.)



Synthèse simple

> "Les indicateurs sont vos balises pour traverser la tempête."



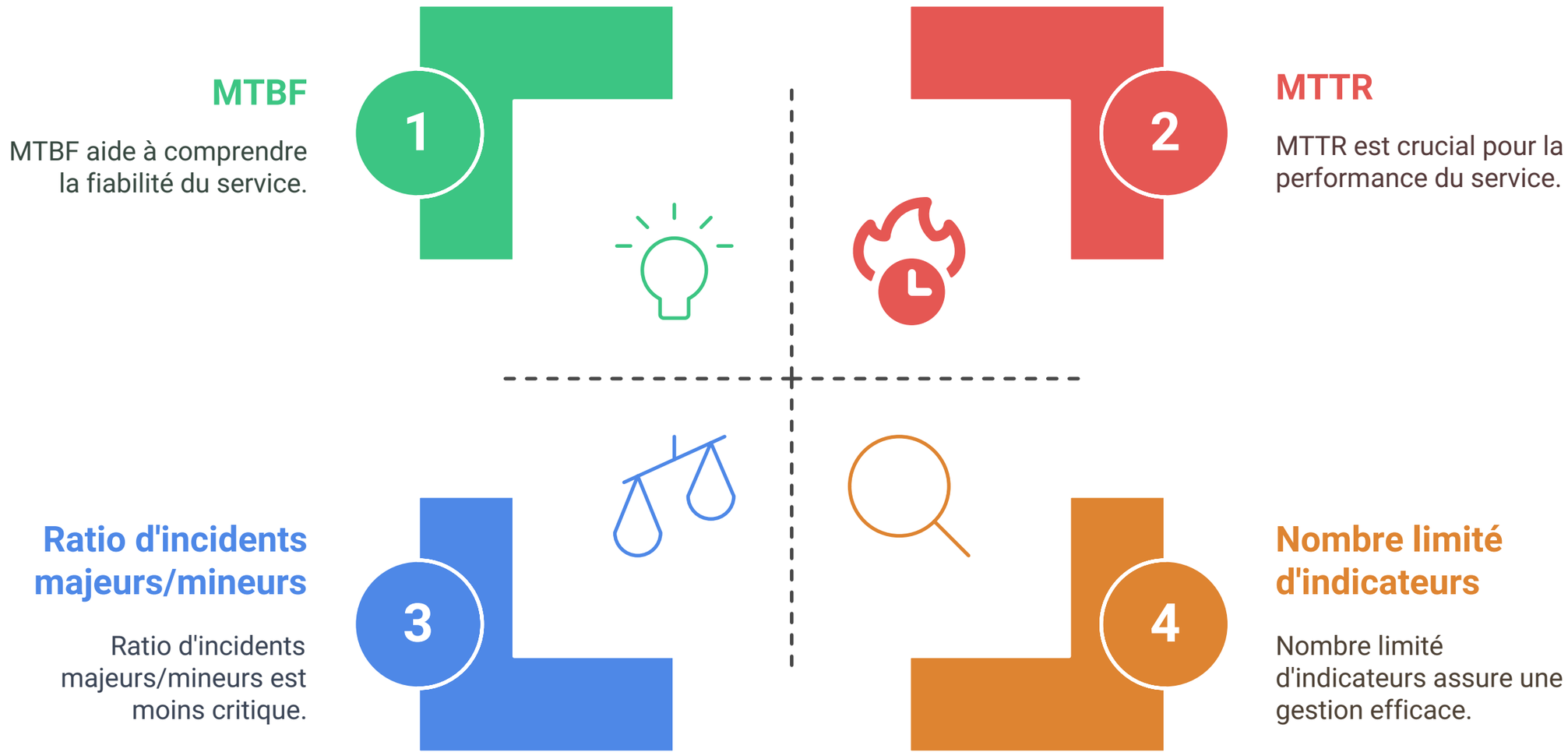
Conseil pratique

- **Ne multipliez pas les indicateurs** inutiles :
- ☒ Visez **5 maximum** par service critique.

- **Suivez en priorité** :

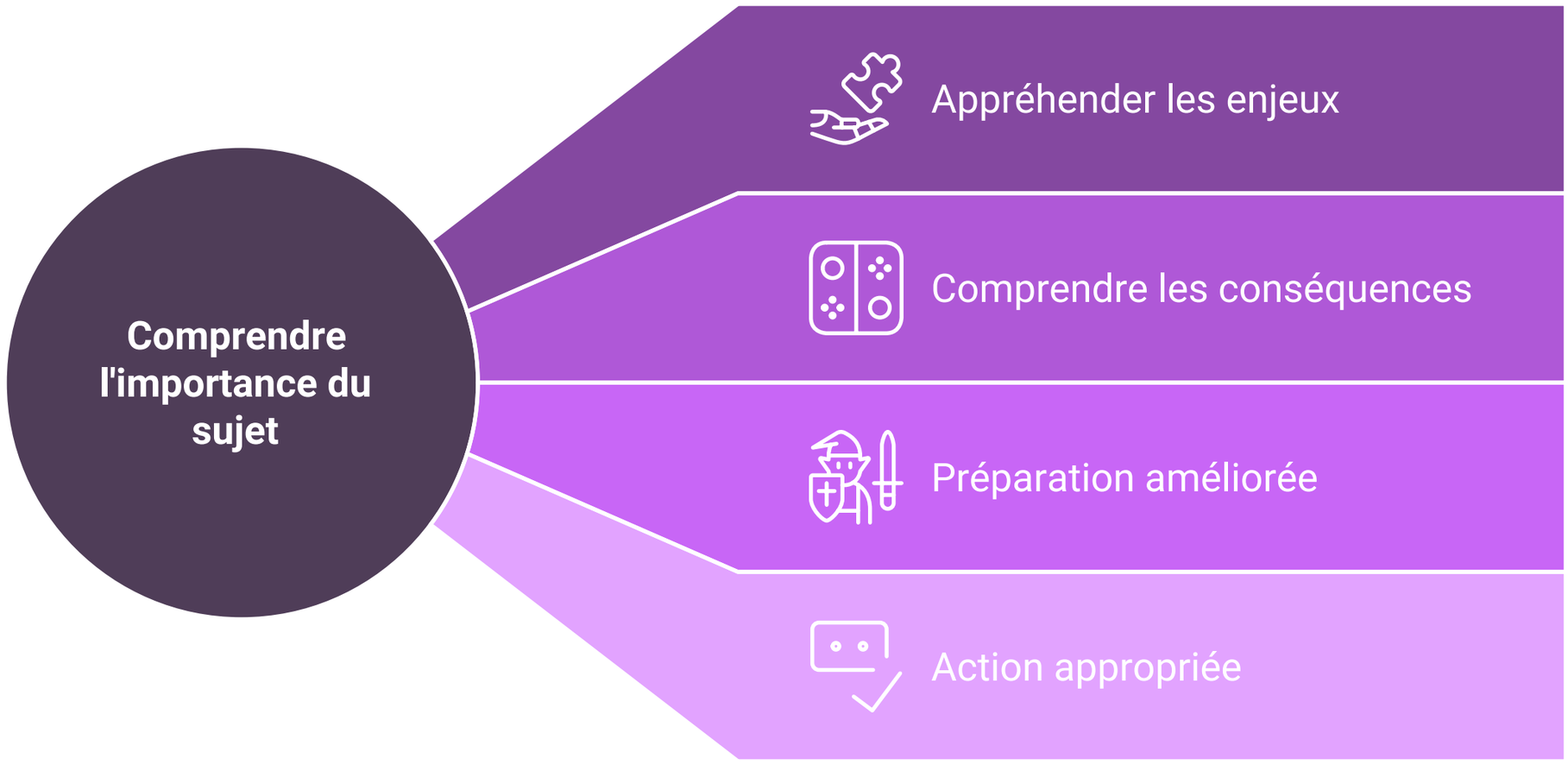
- ☒ MTTR (temps moyen de réparation)
- ☒ MTBF (temps moyen entre deux pannes)

- ☒ Ratio d’incidents majeurs/minorés

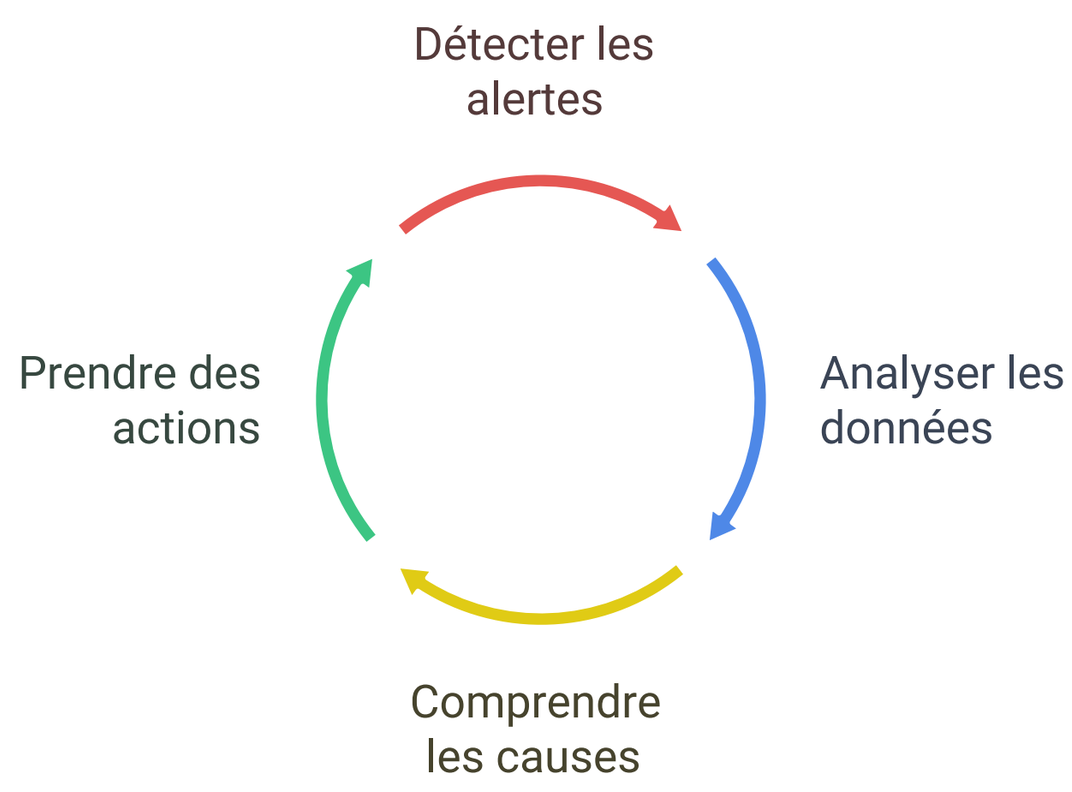


1.1.3 Monitoring vs Observabilité : surveiller vs comprendre

Pourquoi c'est essentiel ?



> "Surveiller sans comprendre, c’est comme avoir une alarme qui sonne… sans savoir où est le feu."



Comparaison illustrée

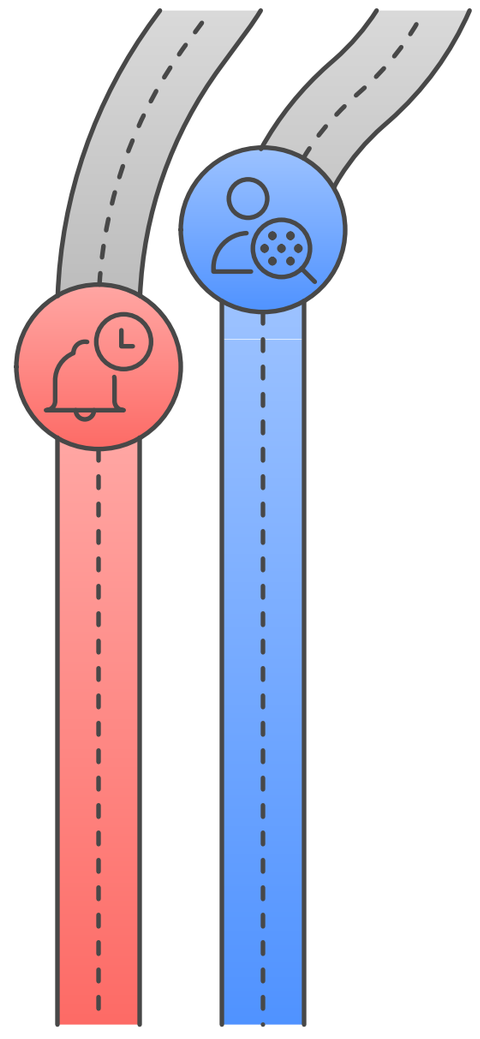
Quelle approche de gestion des systèmes devrions-nous utiliser ?

Surveillance

Idéal pour observer des paramètres connus avec des seuils fixes, comme une alarme de température.

Observabilité

Mieux pour comprendre la dynamique interne et diagnostiquer des problèmes imprévus, comme un médecin.



Synthèse simple

> "**Monitoring** vous alerte sur l’évidence.
>
> **Observabilité** vous éclaire sur l’invisible."

Cycle de surveillance et d'observabilité

Surveiller les événements

Détecter les problèmes évidents

Analyser les données

Comprendre les causes sous-jacentes

Résoudre les problèmes

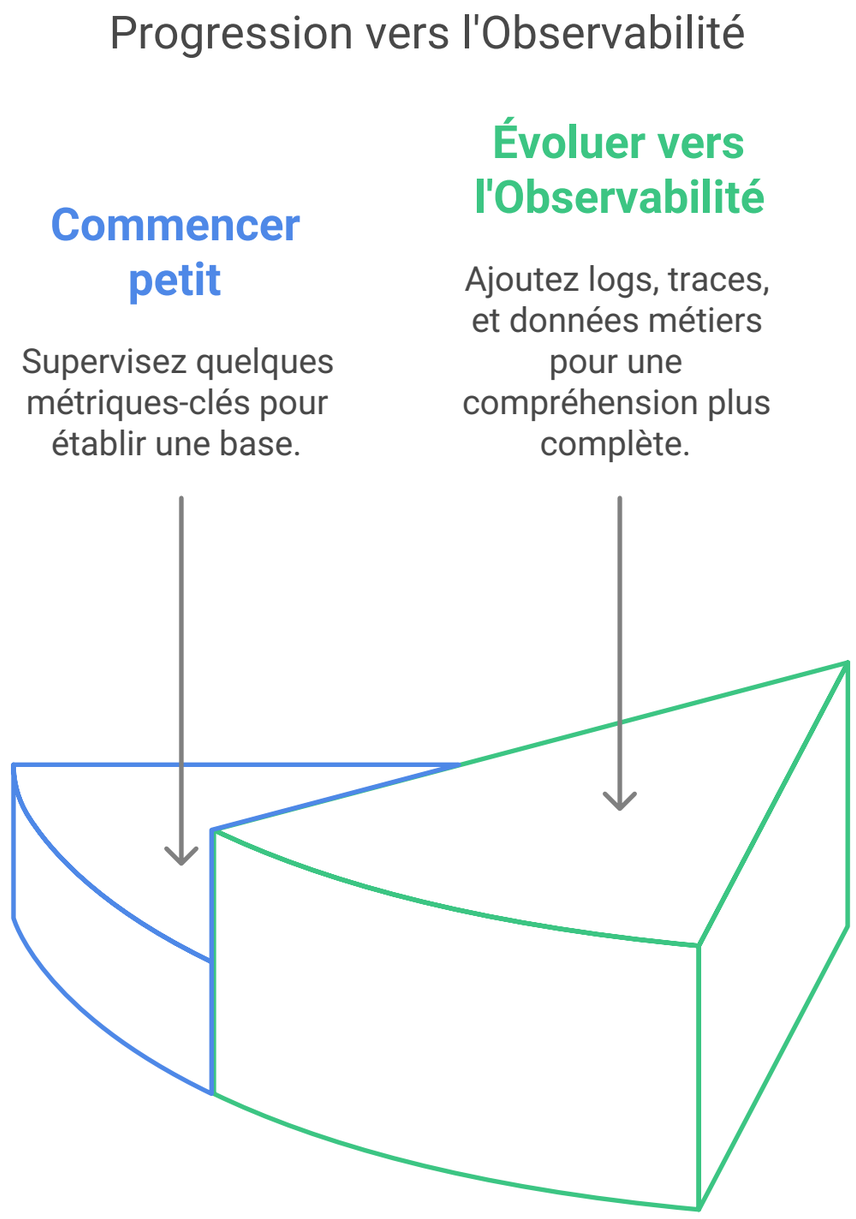
Mettre en œuvre des actions correctives

Améliorer les systèmes

Optimiser pour la résilience

Conseil pratique

- **Commencez petit** : Supervisez quelques métriques-clés.
- **Évoluez vers l'observabilité** : Ajoutez logs, traces, et données métiers.



1.1.4 Les grands cadres méthodologiques : ITIL, NIST, ISO 27001, NIS2, SRE

Pourquoi c'est essentiel ?

> "S’appuyer sur les standards, c’est bénéficier de décennies d'expérience collective."

Adhésion aux normes

Pros

1 Expérience collective

Bénéficier de décennies d'expérience collective en suivant les standards.

2 Meilleures pratiques

Adopter les meilleures pratiques éprouvées par l'expérience.

3 Efficacité accrue

Améliorer l'efficacité grâce à des méthodes standardisées.

Cons

1 Manque de flexibilité

Risque de manque de flexibilité en suivant des normes rigides.

2 Innovation étouffée

Possibilité d'étouffer l'innovation par conformité excessive.

3

Panorama simplifié

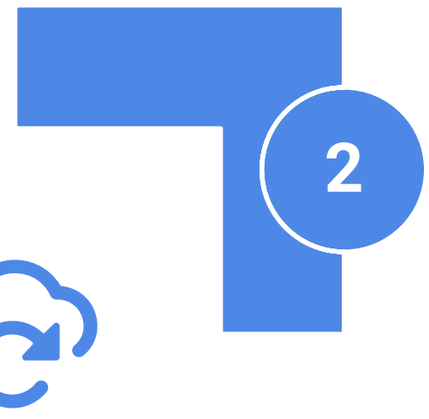
Cadres pour la gestion des incidents et la fiabilité

ITIL v4

ITIL v4 structure les incidents et changements dans les DSI.

SRE

SRE optimise la fiabilité opérationnelle dans les DSI modernes.



NIS2

NIS2 renforce la conformité cyber pour les secteurs critiques.

NIST (SP800-61r2)

NIST guide la réaction aux cyber-incidents dans les SOC.

Synthèse simple

> "Il existe une boîte à outils pour chaque situation. Utilisez-la intelligemment."

Cycle d'utilisation intelligente des outils

Identifier la situation

Reconnaître le problème ou la tâche à accomplir.

Sélectionner les outils appropriés

Choisir les outils les plus pertinents pour la situation.

Appliquer les outils

Utiliser les outils sélectionnés pour résoudre le problème.

Évaluer les résultats

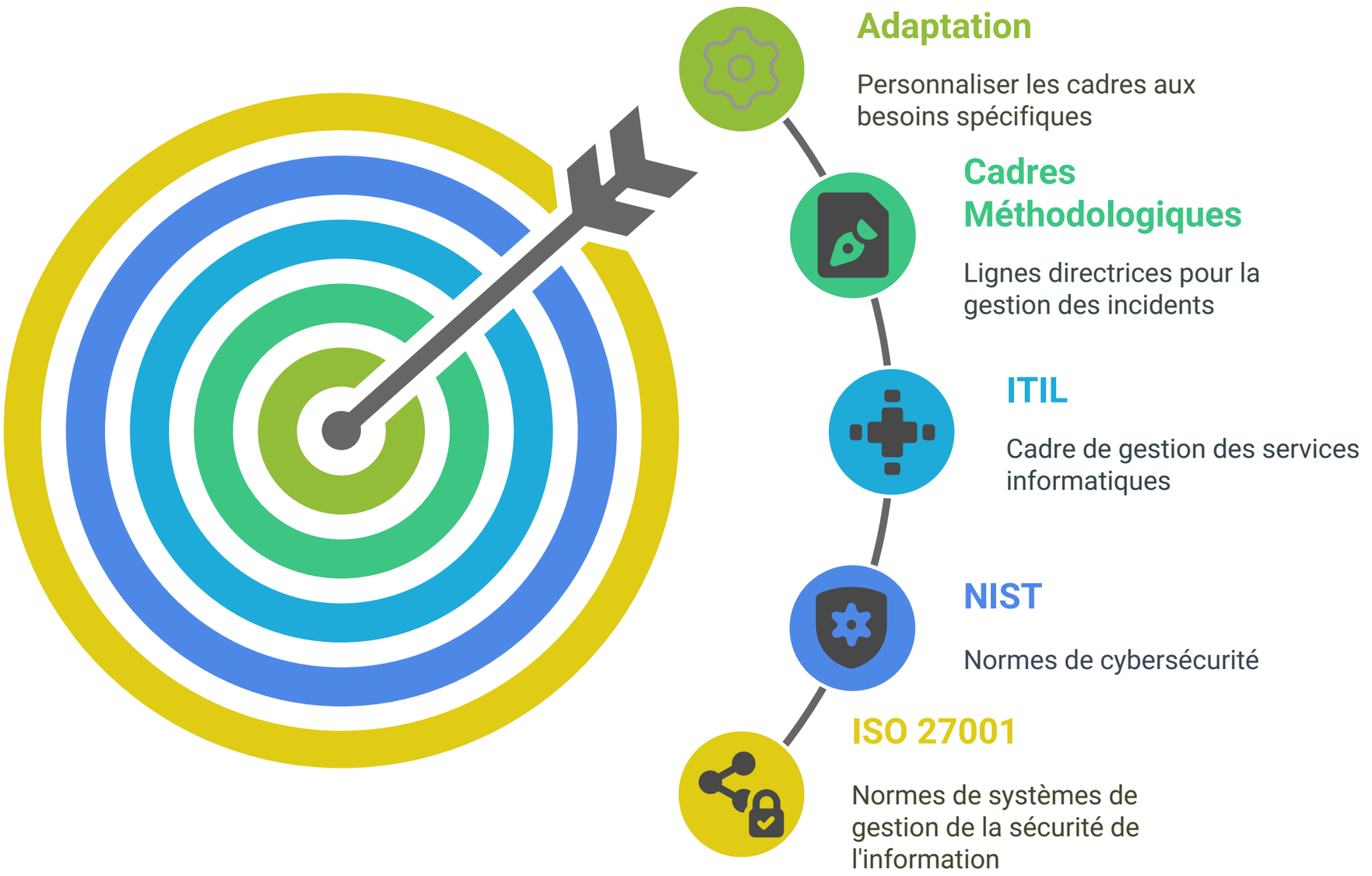
Évaluer l'efficacité des outils utilisés.

Ajuster la stratégie

Modifier l'approche si nécessaire pour de meilleurs résultats.

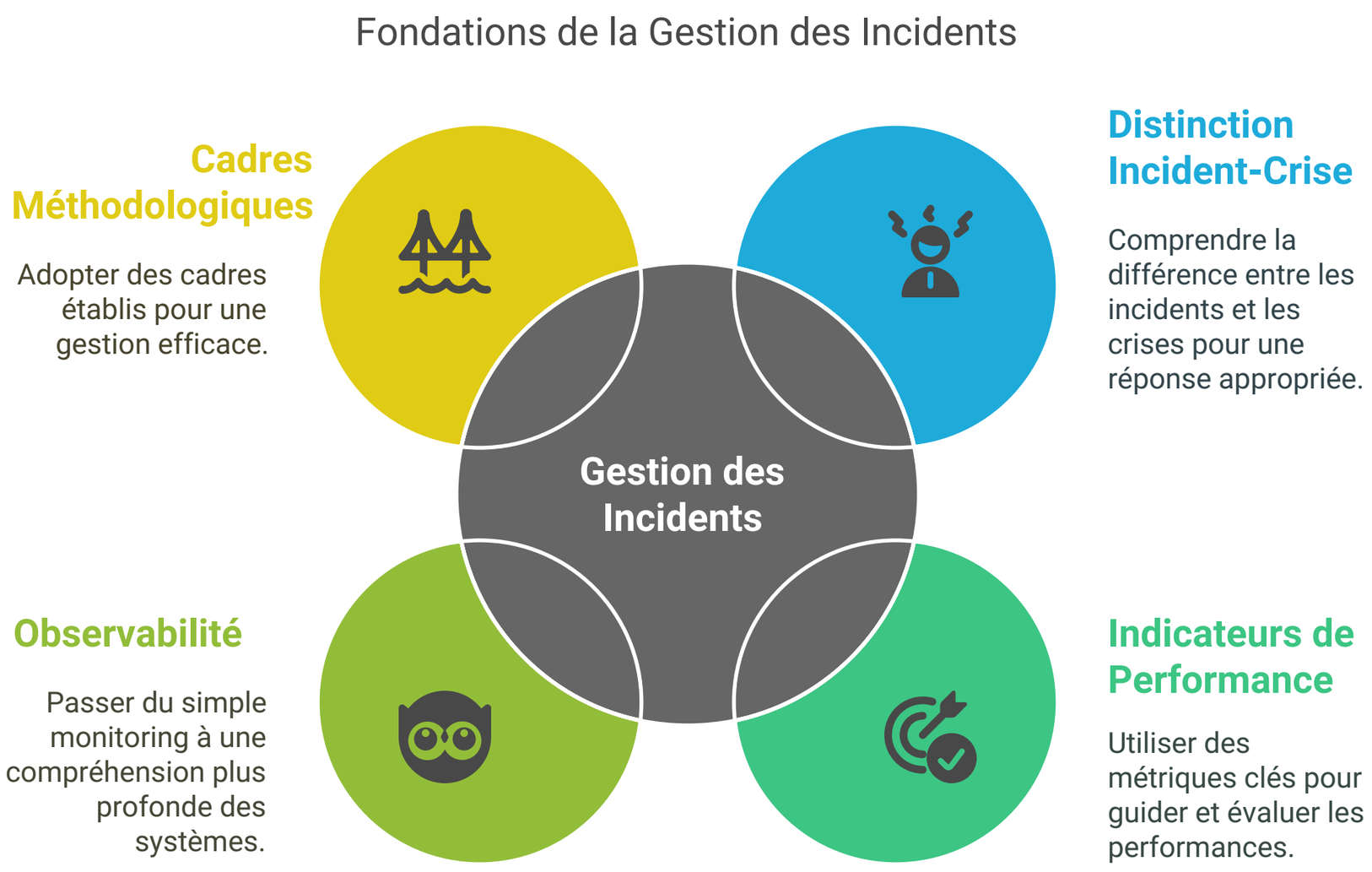
Conseil pratique

- Ne cherchez pas à **tout appliquer** à la lettre.



- **Adaptez** chaque cadre à **votre contexte**, à vos **moyens**, à vos **risques**.

Résumé complet du Chapitre 1.1



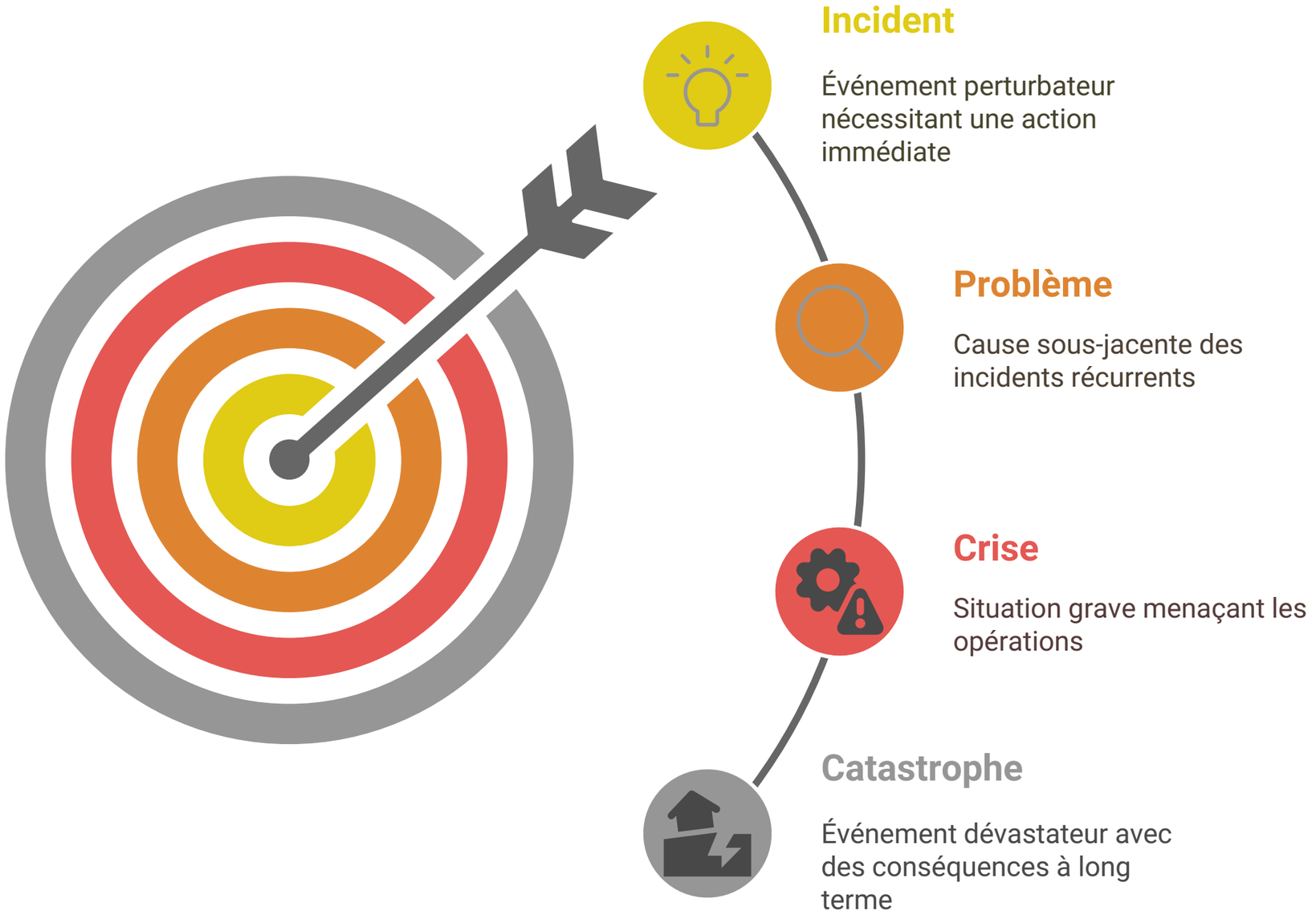
📋 Pour aller plus loin

- **Exercices interactifs** :
  - Classer des cas pratiques (incident ou crise ?)
  - Trouver l’indicateur critique adapté à un service donné
- **Quiz d’ancrage** : 10 questions flash
- **Checklist téléchargeable** : "Bien cadrer son incident management en 10 points"

Bonus possible pour diffusion :

- **Carte mentale** "Les 4 axes de la compréhension Incident Management"

Les 4 axes de la gestion des incidents



Incident

Événement perturbateur nécessitant une action immédiate

Problème

Cause sous-jacente des incidents récurrents

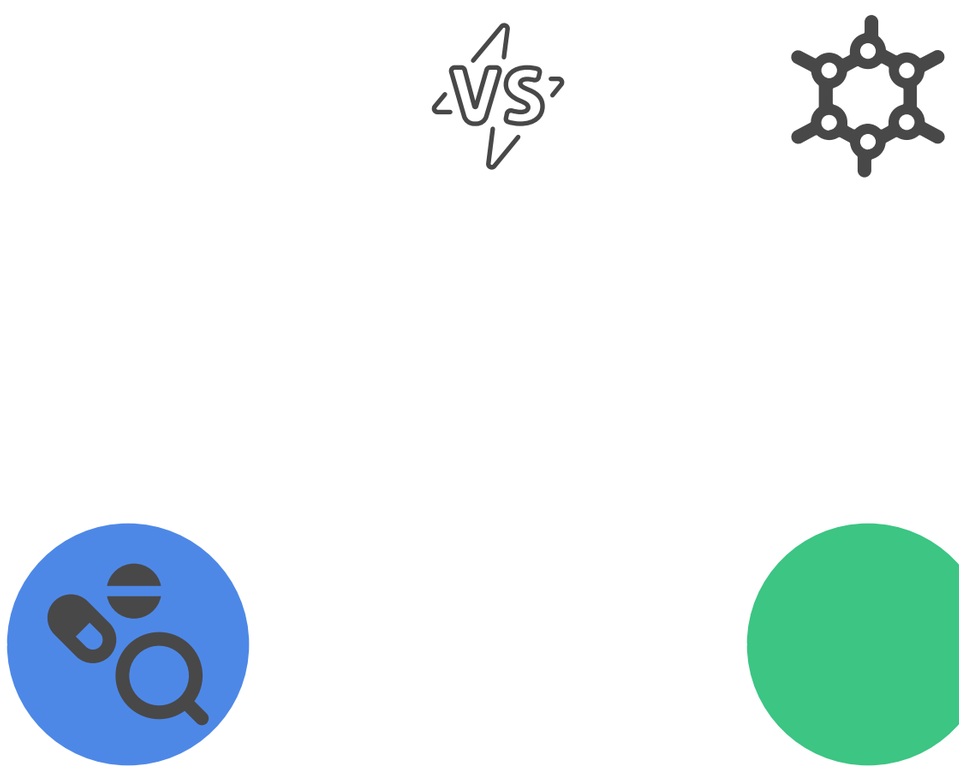
Crise

Situation grave menaçant les opérations

Catastrophe

Événement dévastateur avec des conséquences à long terme

Choisissez la meilleure approche pour la gestion des systèmes et la récupération des données.



Monitoring

Se concentre sur les métriques prédéfinies pour la détection des problèmes

Observabilité

Fournit une compréhension plus approfondie des systèmes grâce à l'exploration des données

- **Vidéo d'animation résumant le chapitre (1 min 30)**