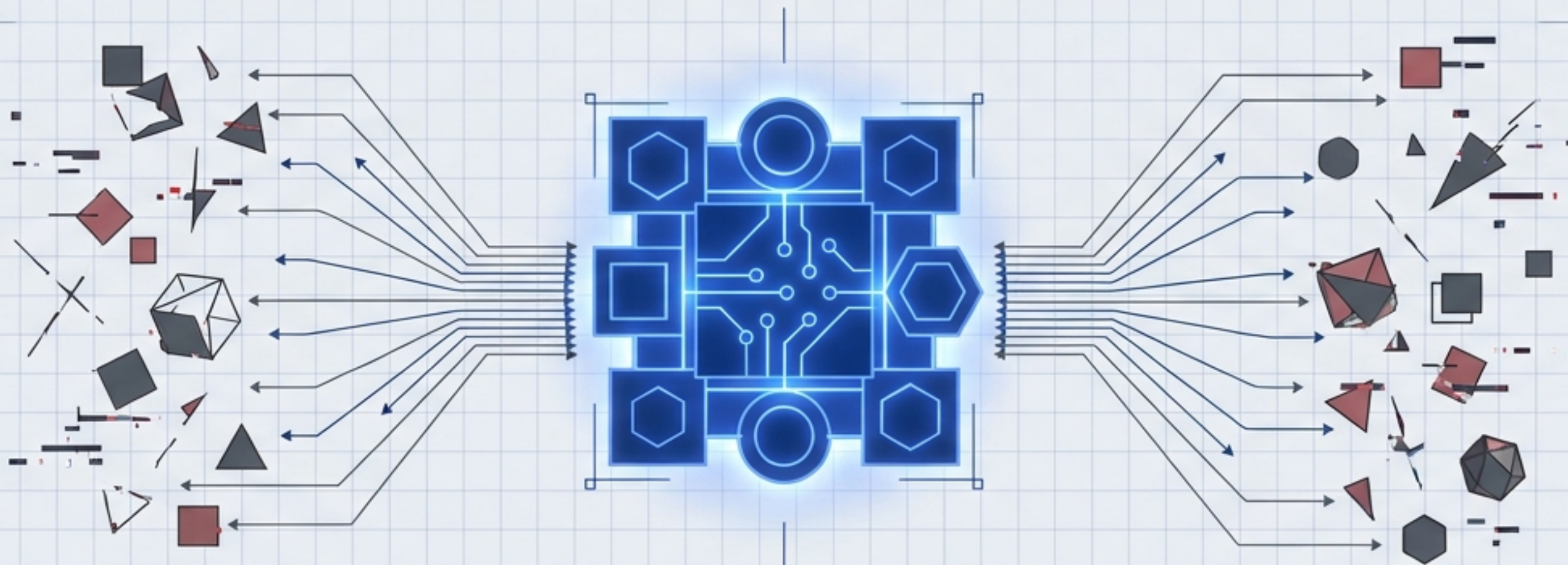


Allumer une bougie plutôt que de maudire l'obscurité

Un référentiel stratégique pour la conception, le développement et l'exploitation d'un Centre d'opérations de sécurité (SOC) mature



AUTEUR :

VERSION :

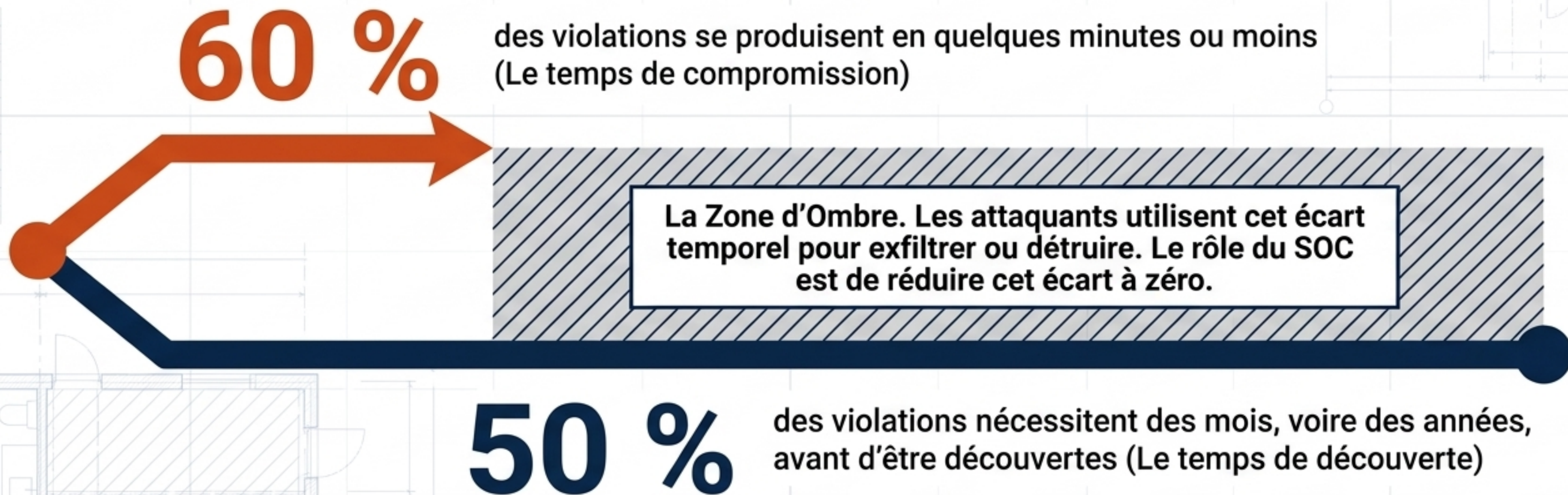
AUTEUR : Équipe d'Architecture SOC

VERSION : Référentiel Principal
STATUT : Actif

PORTÉE DU DOCUMENT :
- Paysage des menaces
- Gestion des risques
- Réponse aux incidents

Une compromission informatique n'est plus une question de « si », mais de « quand »

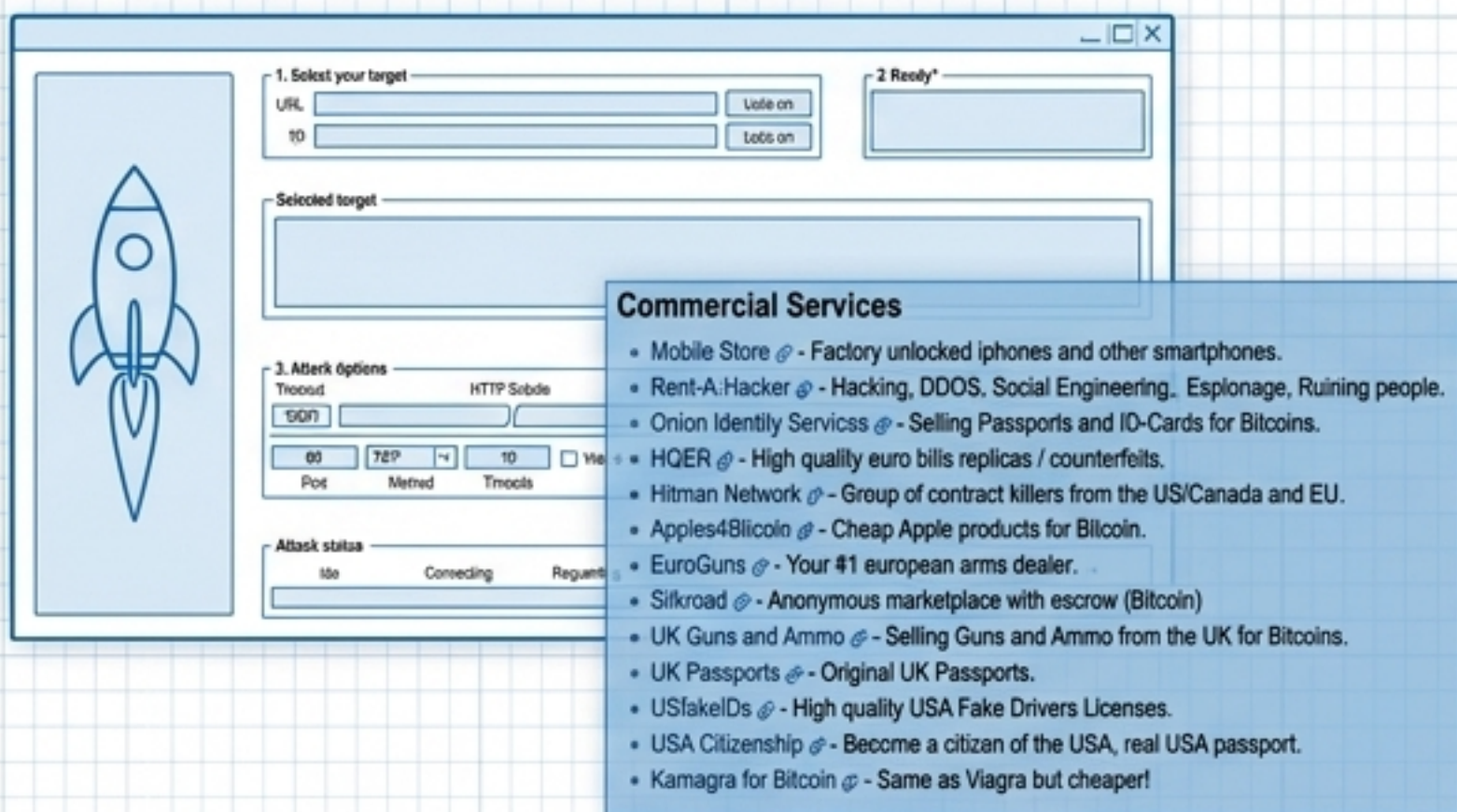
« Il existe deux types d'entreprises : celles qui ont été piratées et celles qui ignorent encore qu'elles l'ont été. » — John Chambers, ancien PDG de Cisco Systems.



La collision entre l'industrialisation des menaces et l'expansion des surfaces d'attaque

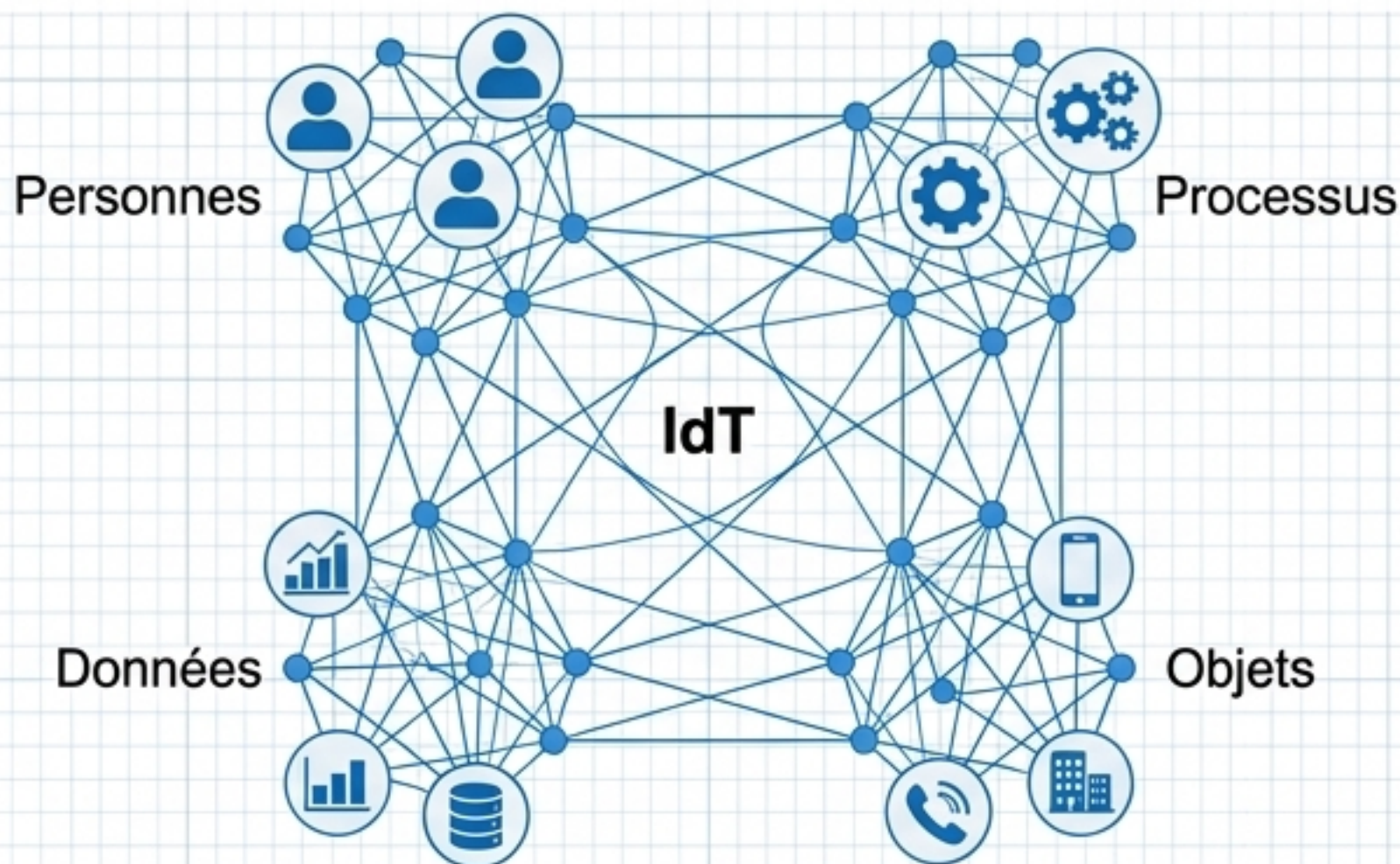
Démocratisation de l'offensive

Des outils automatisés sophistiqués transforment des novices (« script kiddies ») en menaces sérieuses. Le jeu du chat et de la souris annule les solutions miracles (ex: contournement des miracles (ex: contournement des bacs à sable).

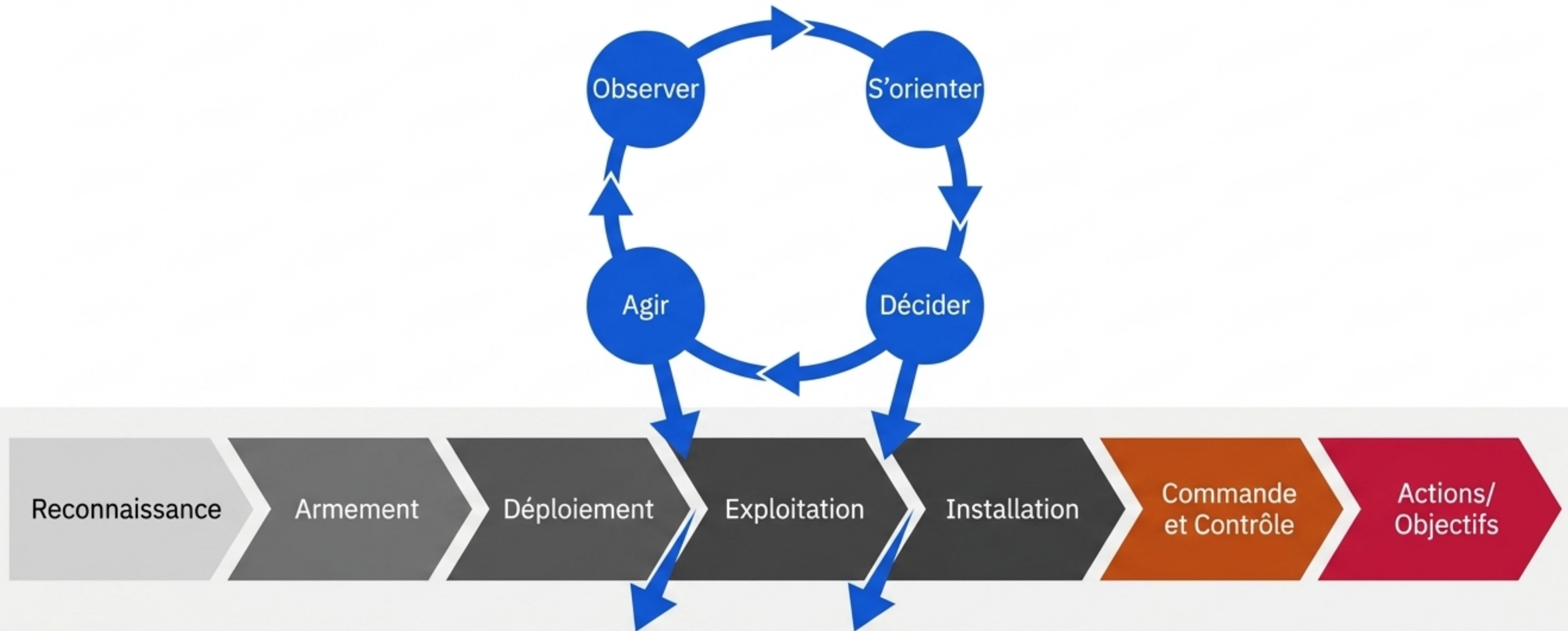


Complexité des affaires

La surface à défendre s'étend au-delà du réseau traditionnel à travers la migration vers le cloud, la prolifération du BYOD et les exigences strictes de conformité (PCI DSS, ISO 27001).



L'anatomie de l'affrontement : Intercepter la chaîne d'attaque



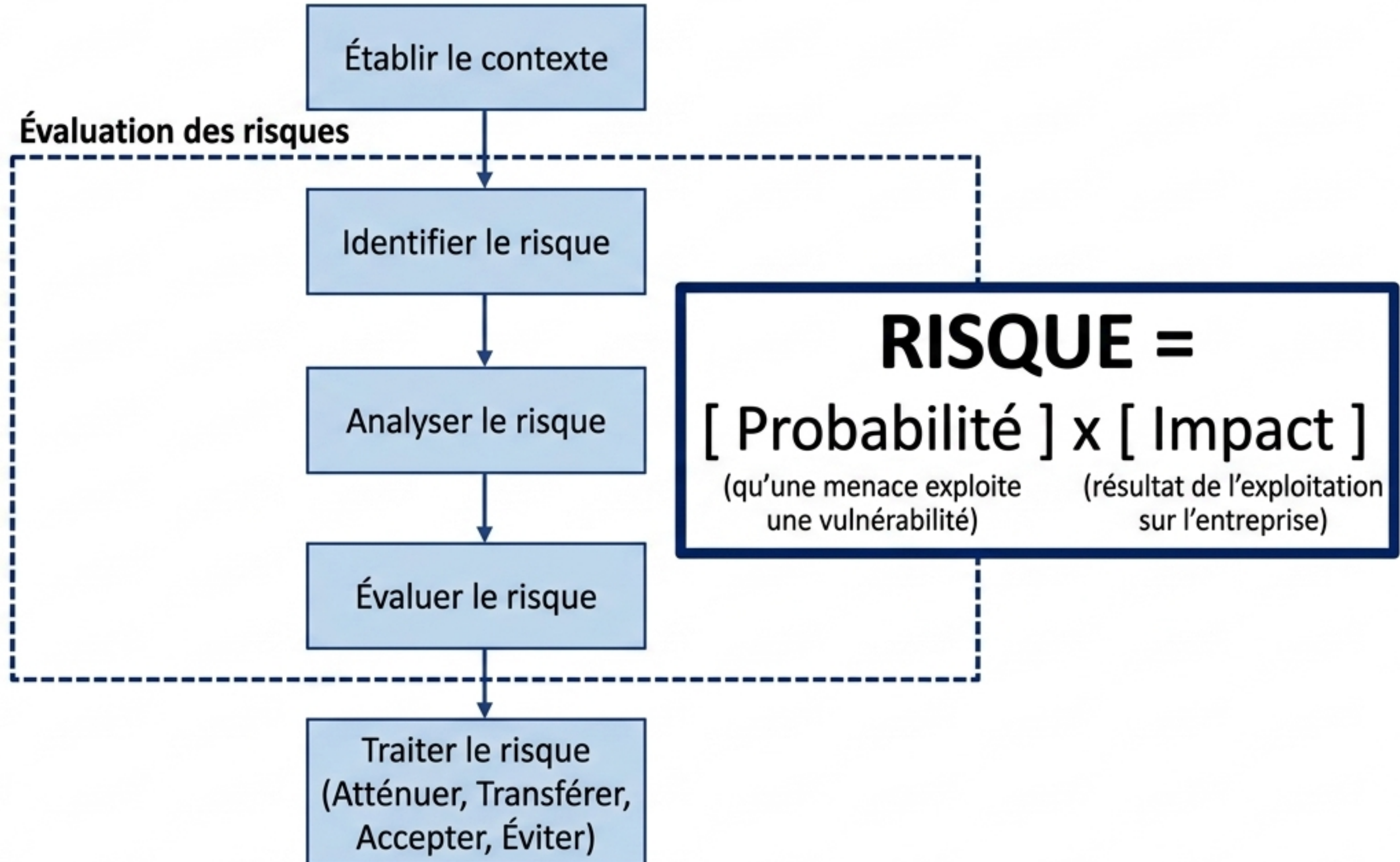
Le SOC n'est pas un ensemble d'outils. C'est l'incarnation opérationnelle de la boucle OODA, conçue pour intercepter et neutraliser l'attaquant avant la phase 7.

La gestion des risques dicte l'urgence et la nature de la réponse

Concepts Clés

L'**Assurance de l'Information** (IA) est le cadre global visant à gérer les risques et garantir la confiance.

La **Sécurité de l'Information** (InfoSec) est le sous-ensemble tactique protégeant techniquement les systèmes.



Traduire l'incertitude en priorité : La carte thermique des risques

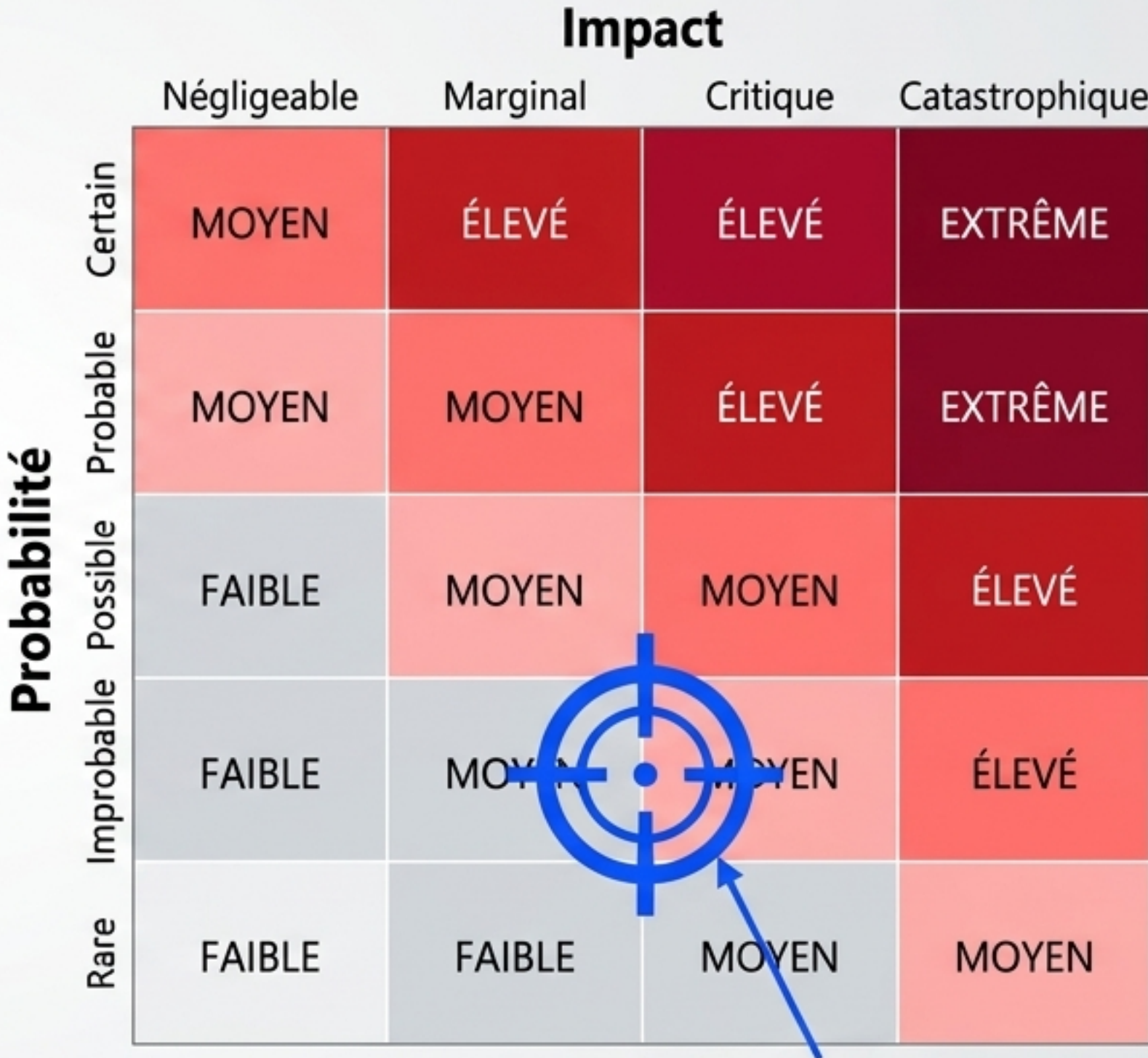
Incident Brief

Scénario d'Évaluation (OCTAVE)

- **Événement** : Nouvelle vulnérabilité annoncée.
- **Cible** : Actif interne critique (non connecté à Internet).
- **Contrôle existant** : Pare-feu limitant l'accès aux utilisateurs internes.

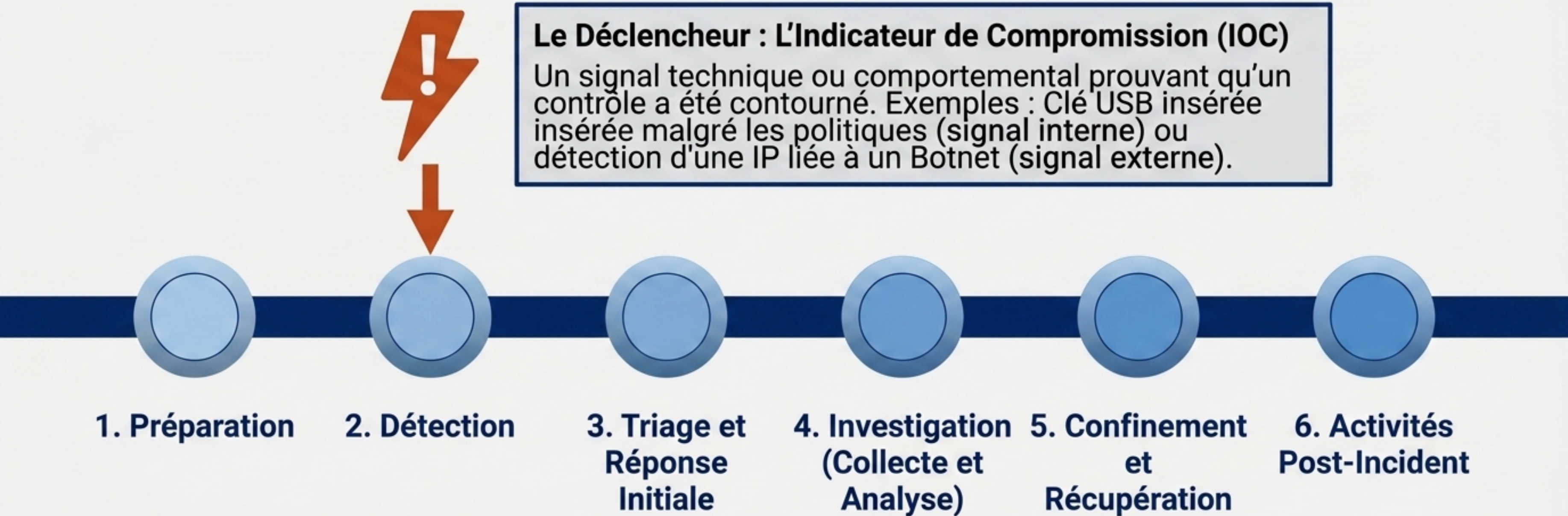
Probabilité : IMPROBABLE (Unlikely)

Impact : CRITIQUE (Critical)

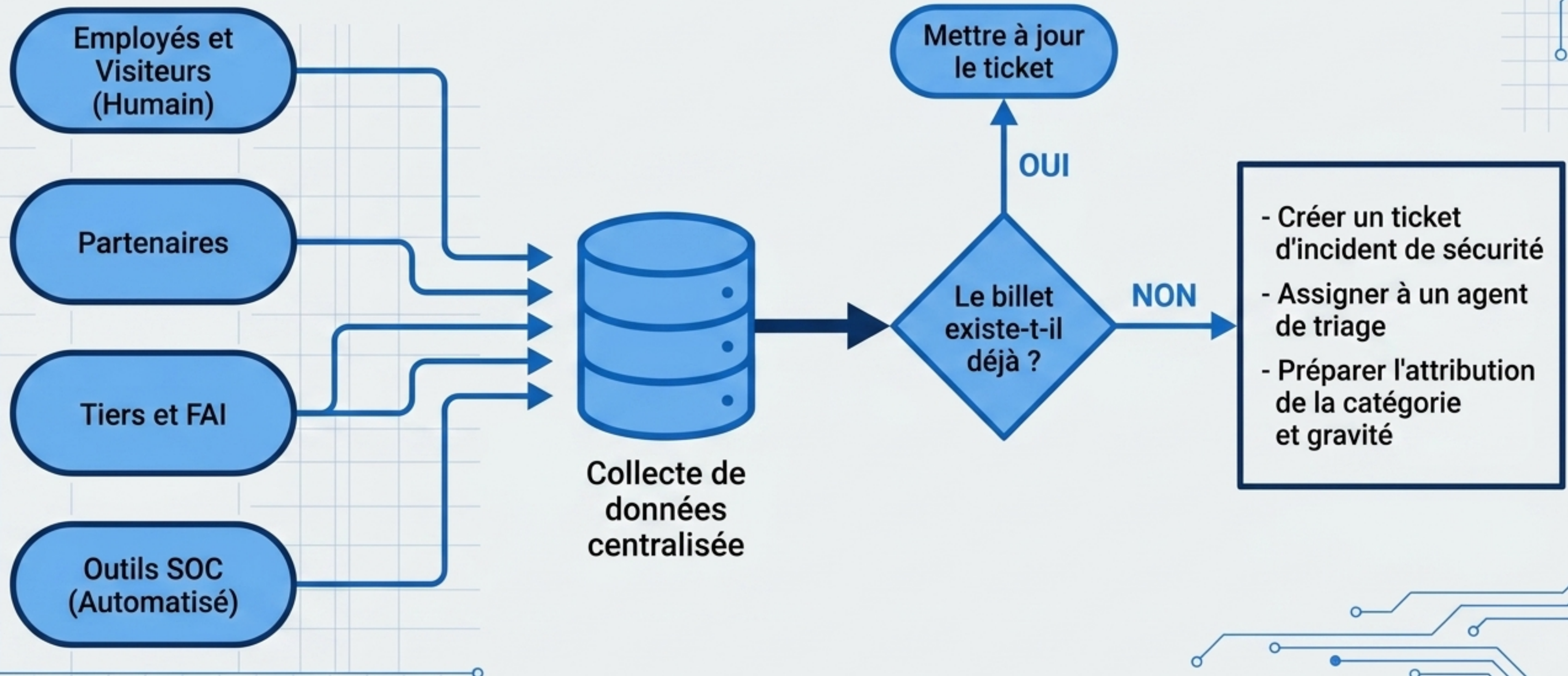


Action modérée planifiée
(gestion des correctifs standard)

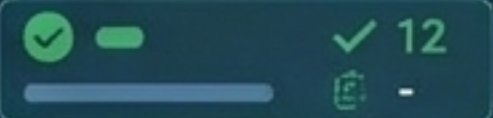
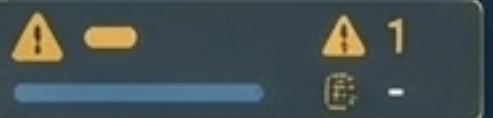
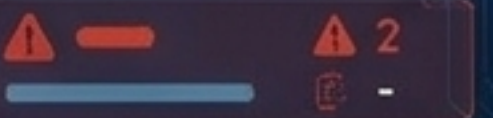
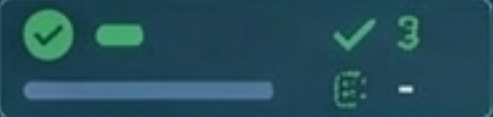
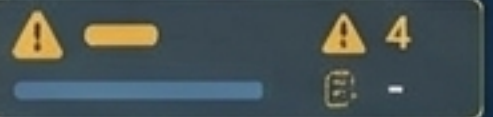
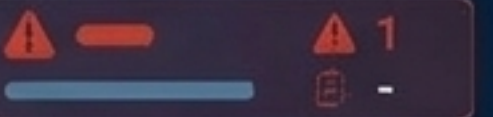
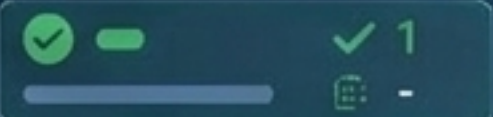
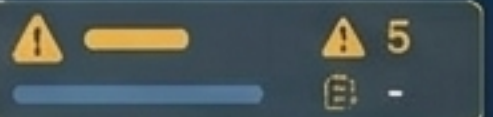
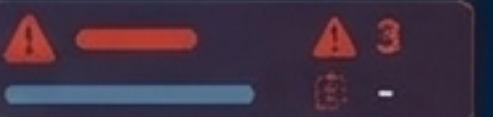
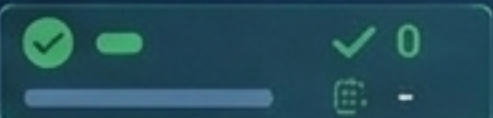
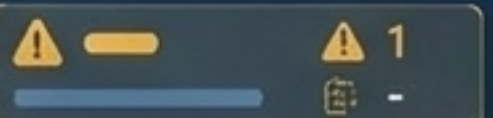
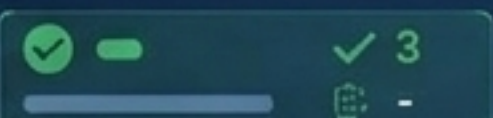
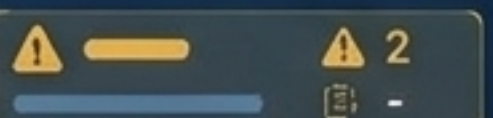
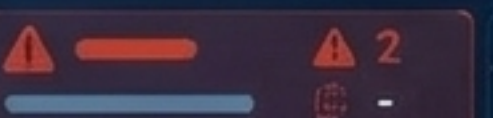
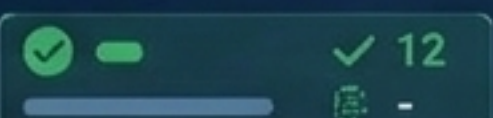
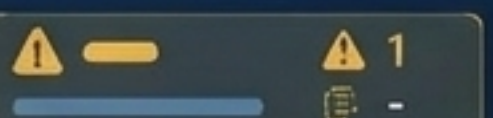
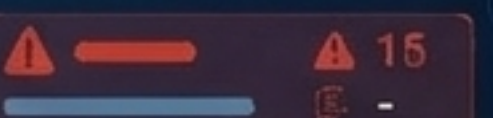
Le moteur opérationnel du SOC : Le cycle de vie d'un incident



Phase 1 - Détection : Capter et centraliser le signal parmi le bruit



Phase 2 - Triage : Triage initial et diagnostic de l'alerte

	Faible (Impact minimal potentiel)	Moyen (Impact significatif potentiel)	Élevé (Impact grave sur les opérations)
0 : Exercice			
1 : Accès non autorisé			
2 : Déni de service (DoS)			
3 : Code malveillant			
4 : Scans et Sondes			
5 : Investigation			

Questions de qualification du gestionnaire d'incidents :

- ☐ L'incident est-il dans le périmètre ?
- ☐ Est-il lié à un événement passé ?
- ☐ Quelle catégorie et gravité ?
- ☐ Qui doit enquêter ?
- ☐ Quel est le délai de résolution ?

Phase 3 - Investigation : Identification de la cause première et escalade

Objectifs de l'Analyse SOC



1. Identifier les systèmes et comptes compromis.



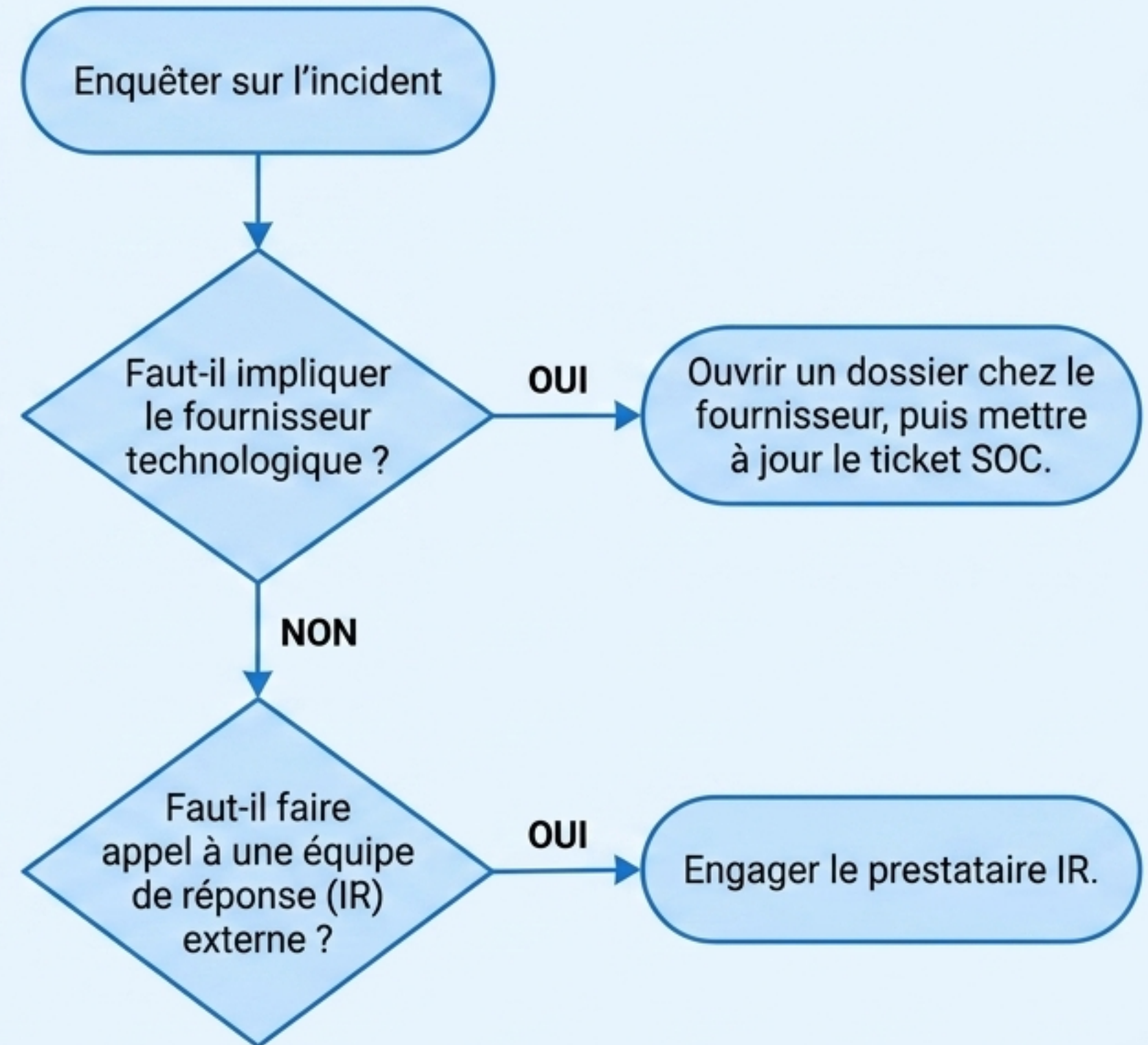
2. Comprendre l'impact réel de l'incident.



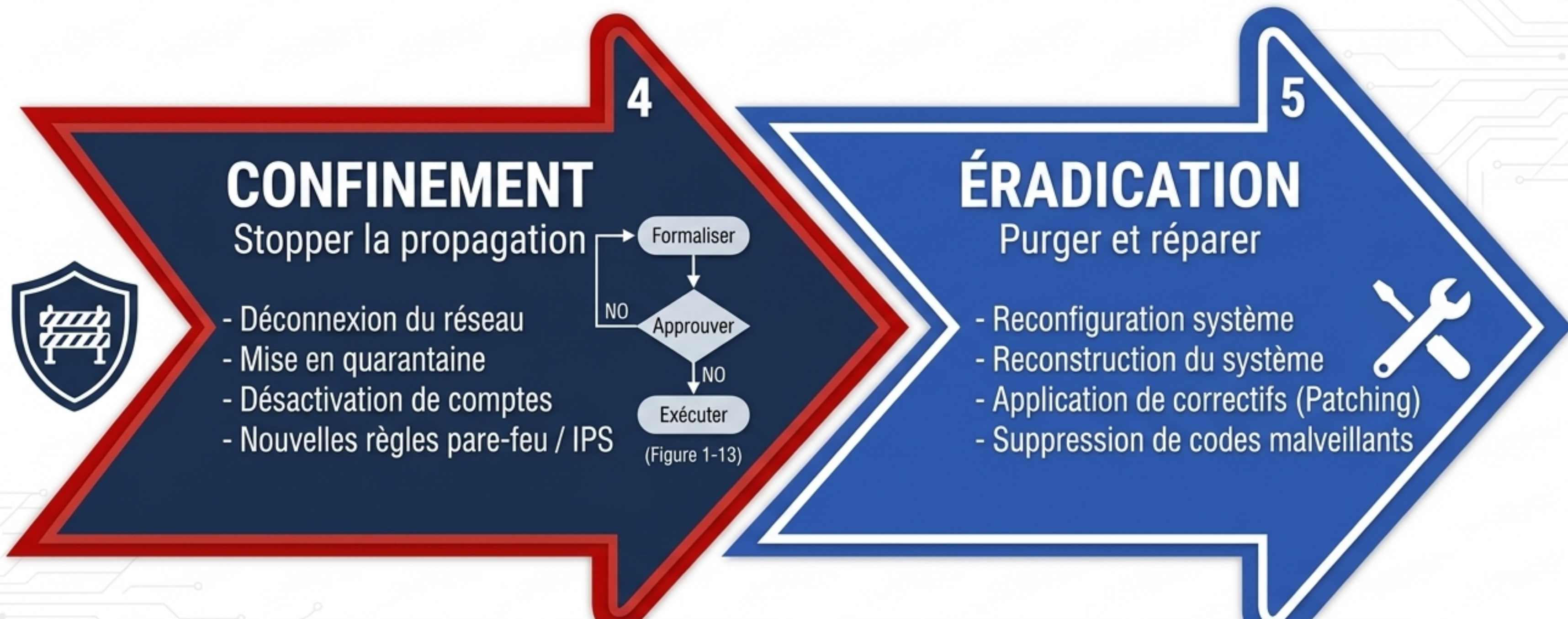
3. Repérer les tentatives d'accès aux données.



4. Reconstruire la chaîne d'événements (Cause première).



Phases 4 & 5 - Confinement et Éradication : Arrêter l'hémorragie et purger



NOTE TACTIQUE : Ces deux phases se chevauchent presque toujours dans la pratique pour minimiser le temps d'arrêt des opérations.

Phase 6 - Post-Incident : Leçons apprises et évolution de la défense

Boucle OODA
(Observer / S'orienter)

Matrice de Risques
(Mise à jour des probabilités)

**L'incident devient une
intelligence exploitable.**

La documentation post-incident sert à améliorer les capacités du SOC de manière proactive :

- Mise à jour des signatures de sécurité.
- Formation ciblée des employés.
- Révision des processus de réponse.

**Analyse
Post-Incident**
(Données de l'attaque,
faillles découvertes)

L'Architecture de la Résilience : Le modèle opérationnel complet du SOC

CONFORMITÉ ET GESTION DES RISQUES

PERSONNES

- Sensibilisation, analystes de sécurité, gestionnaires de triage, experts de conformité.

PROCESSUS

- Boucle OODA, Méthodologie de Réponse aux Incidents (6 phases),
- Évaluation OCTAVE.

TECHNOLOGIE

- Outils de détection, Pare-feu, IPS, Environnements Cloud sécurisés,
- Intelligence centralisée.

Un SOC performant intègre harmonieusement ces trois éléments pour transformer le chaos d'une compromission inévitable en un événement géré, mesuré et neutralisé.
La bougie est allumée.