

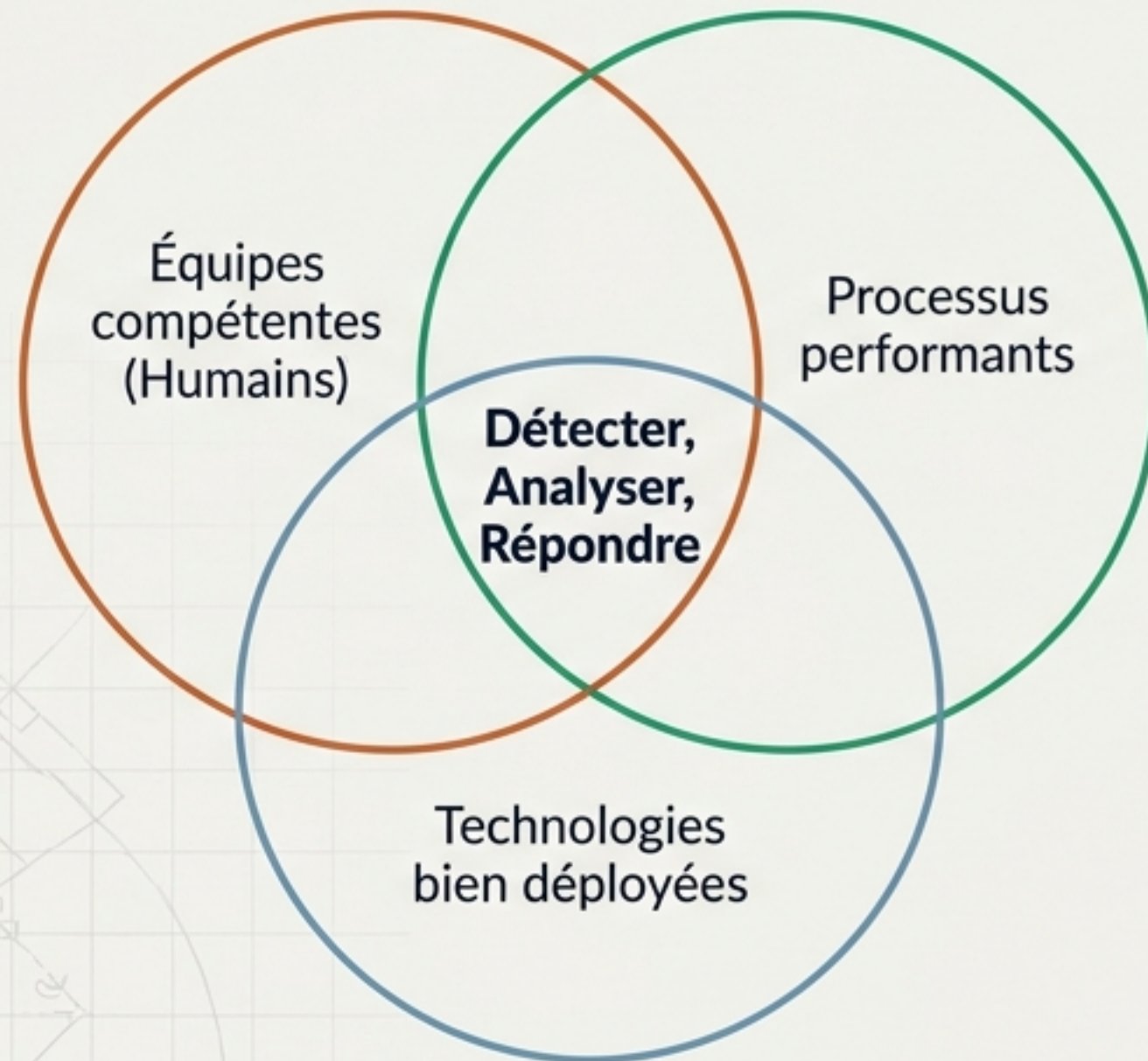
Manuel Tactique du SOC : Réagir aux Événements et Incidents

Cadres méthodologiques, écosystème de collaboration et gestion de l'investigation pour les centres de cyberdéfense.

Statut : Opérationnel | **Classification** : TLP:AMBER | **Révision** : 2.0

“ Ce n’est pas le stress qui nous tue,
c’est notre réaction face à lui. ”

— Hans Selye



Cadre de référence opérationnel

- SOC Modèle de référence
- Niveau 1 (surveillance 24/7) : Imparti à un tiers
- Niveau 2 (investigation) : Interne
- Niveau 3 (réponse/forensique) : Interne relevant du RSSI

Iceberg de Visibilité

Détections Systémiques (SIEM)

Seul un tiers (1/3) des incidents informatiques mondiaux sont détectés par les SIEM.

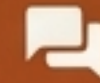
Le Principe d'Inclusion

Un événement n'est pas qu'un journal automatisé. L'humain reste le meilleur capteur du SOC. Se concentrer uniquement sur le SIEM garantit de manquer des incidents critiques.

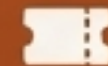
Ligne de Démarcation Technique

Signalements Humains et Opérationnels

Courriels

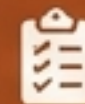


Messagerie instantanée



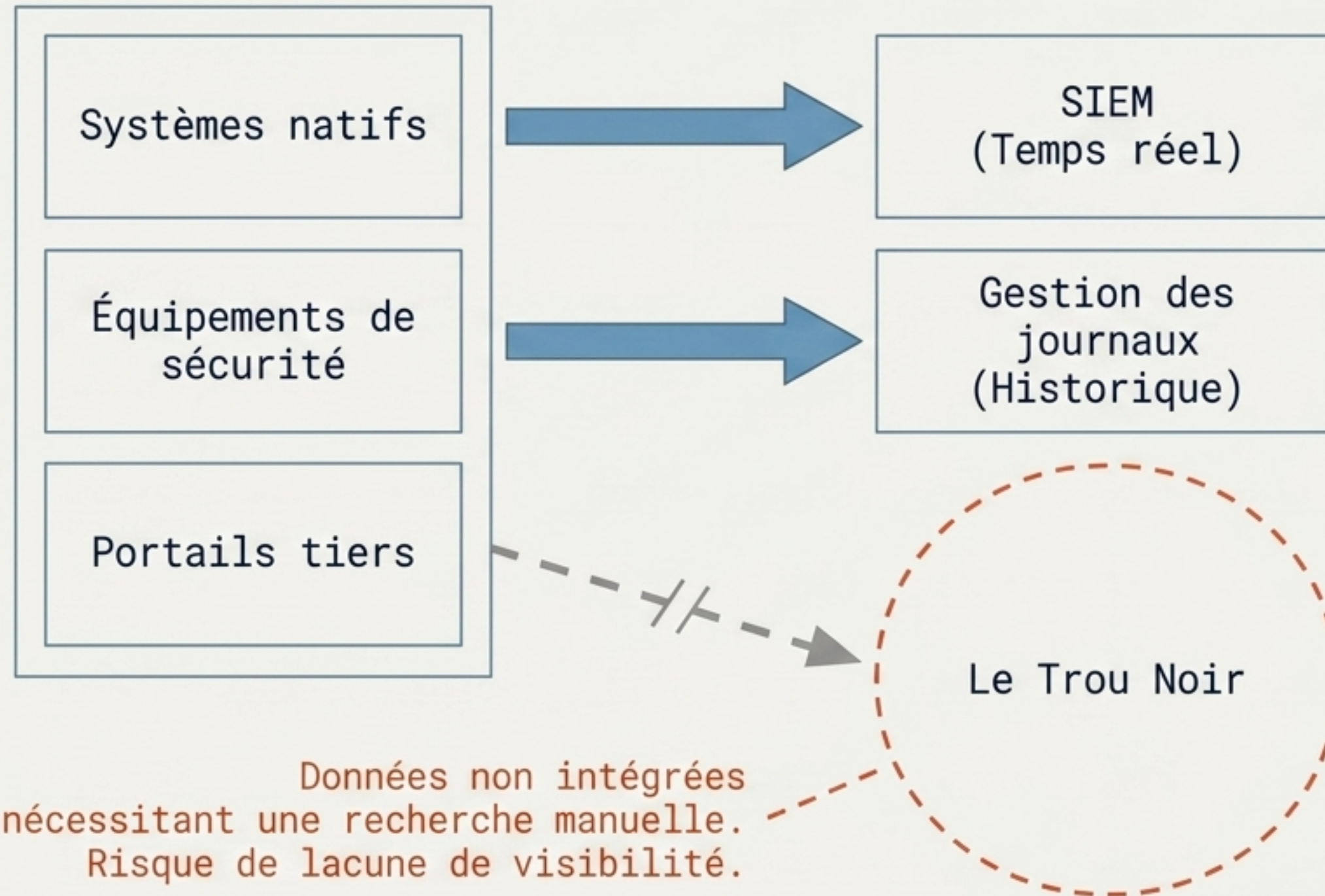
Billets de service (ITSM)

Appels téléphoniques



Contrôles de routine

L'Architecture d'Acquisition



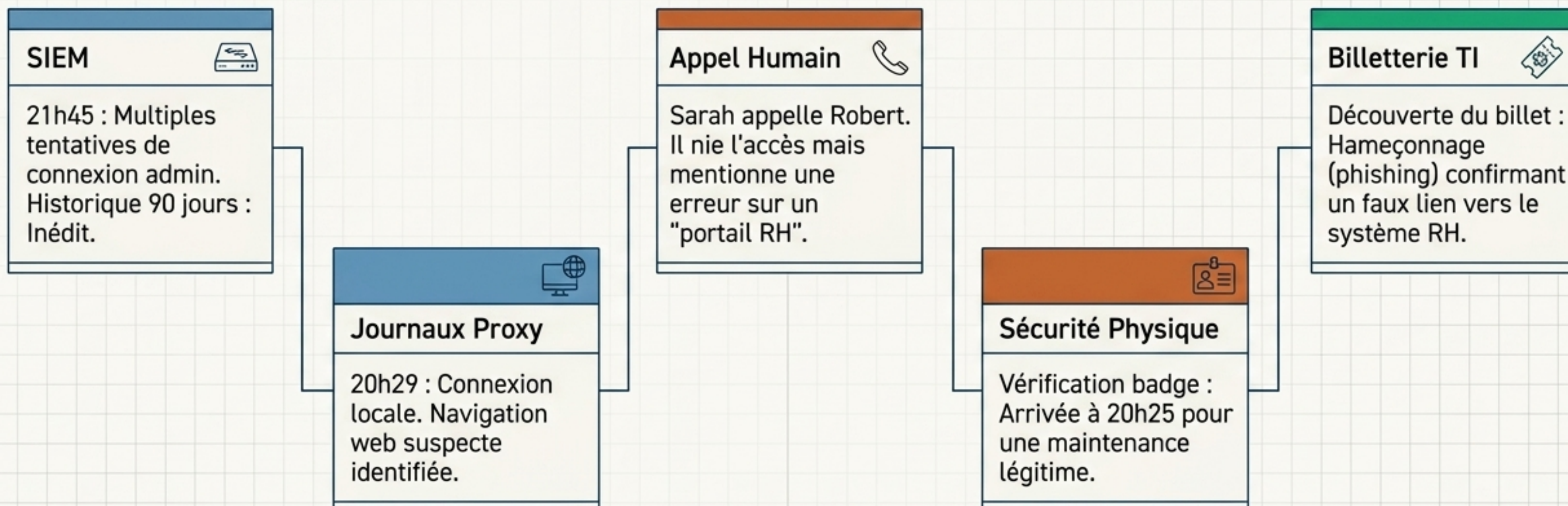
Data Card

Dossier 404 : L'infection de Robert

L'alerte initiale

- Mardi, 21h45.
- Alerte SIEM Priorité Haute.
- Le compte de Robert (Admin Système) tente des connexions à des systèmes critiques inhabituels.
- Sarah (Analyste SOC Niveau 2) prend en charge l'alerte.

Chronologie de l'Investigation



L'investigation de première ligne exige de recouper des journaux techniques normalisés avec des données comportementales et physiques non intégrées.

La Matrice de Taxonomie des Incidents

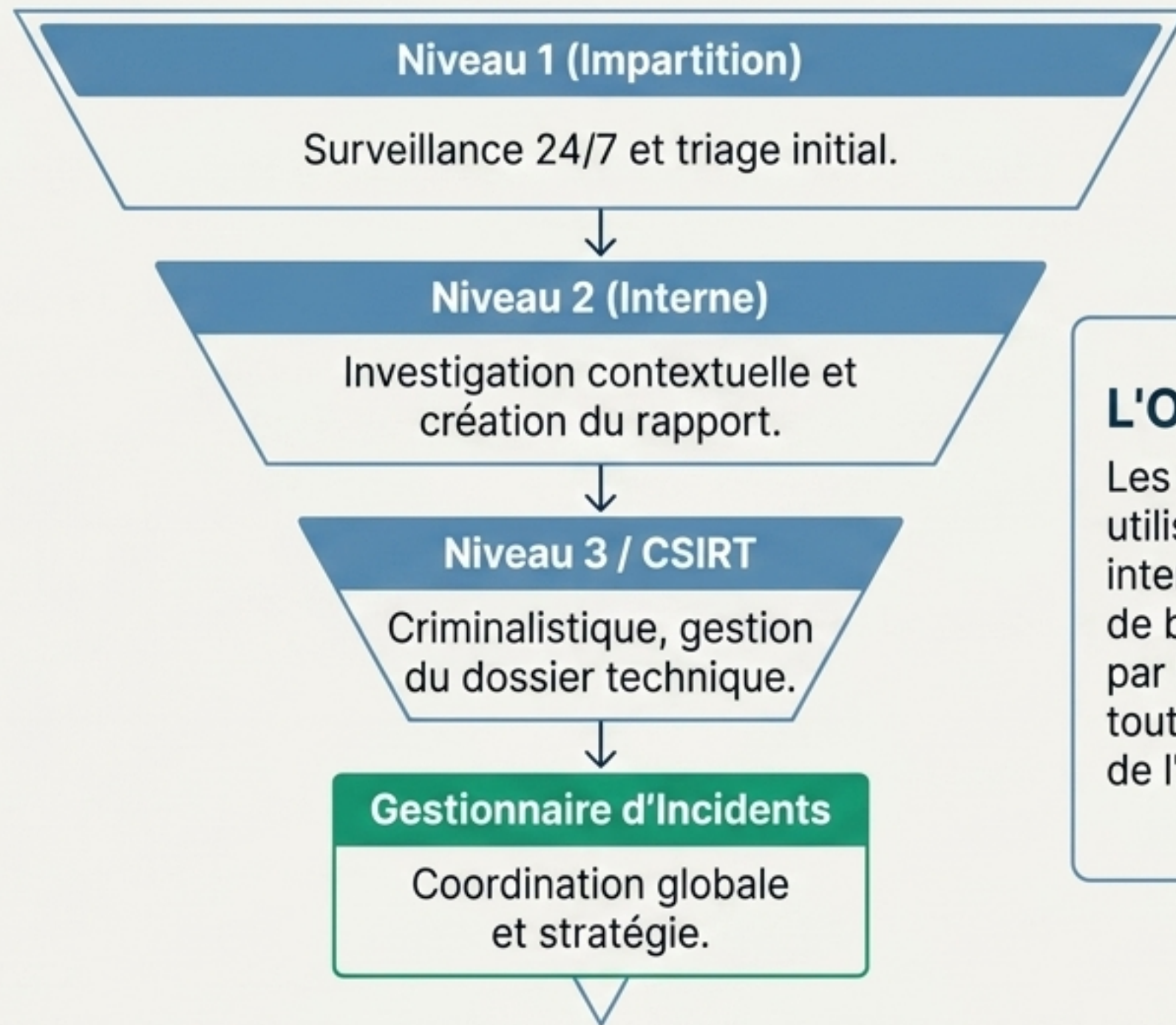
La Matrice de Taxonomie des Incidents			
Concept	Source Typique	Définition / Seuil	Action Requise
Événement	Système / Humain	Artefact indiquant qu'un phénomène s'est produit.	Acquisition et corrélation.
Faux Positif	Règle SIEM erronée	Alerte déclenchée de manière inappropriée.	Ajustement des règles.
Rapport d'incident	Analyste (Niveau 2)	Signalement d'un événement grave justifiant enquête.	Soumission à la gestion des cas.
Dossier (Case)	Équipe CSIRT	Enveloppe regroupant les événements liés.	Application de méthodologies.
Incident	Enquêteur	Série d'événements avérés avec conséquences néfastes.	Déclaration officielle, remédiation.

Data Card

Changement de statut

- Validation des faits par Sarah.
- Faux positif écarté.
- Création d'un Rapport d'incident avec journaux et captures d'écran joints.
- Alerte transmise à l'équipe de Niveau 3 (CSIRT).

Modèle de l'Escalade Structurée



L'Outil Silencieux

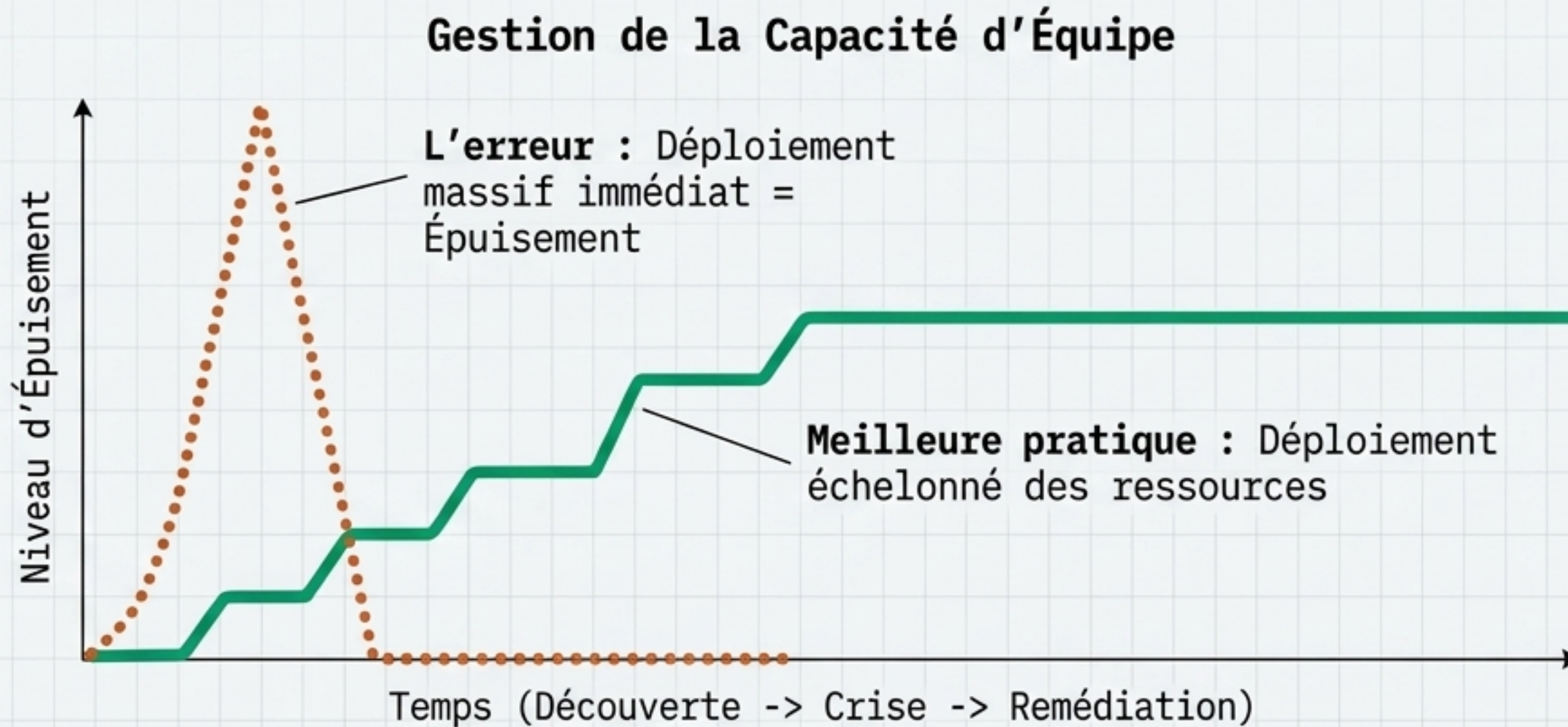
Les analystes doivent utiliser une messagerie interne avec chiffrement de bout en bout gérée par le SOC pour éviter toute interception lors de l'investigation.

Dossier 404

Ouverture du Cas

- Dan (CSIRT, Niveau 3) reçoit l'alerte.
- Échanges via messagerie sécurisée avec Sarah.
- Le rapport devient un Cas officiel.
- Demande de traçage du courriel (Spear Phishing).
- Lancement des analyses de vulnérabilités.

Gestion de la Capacité d'Équipe



Data Card

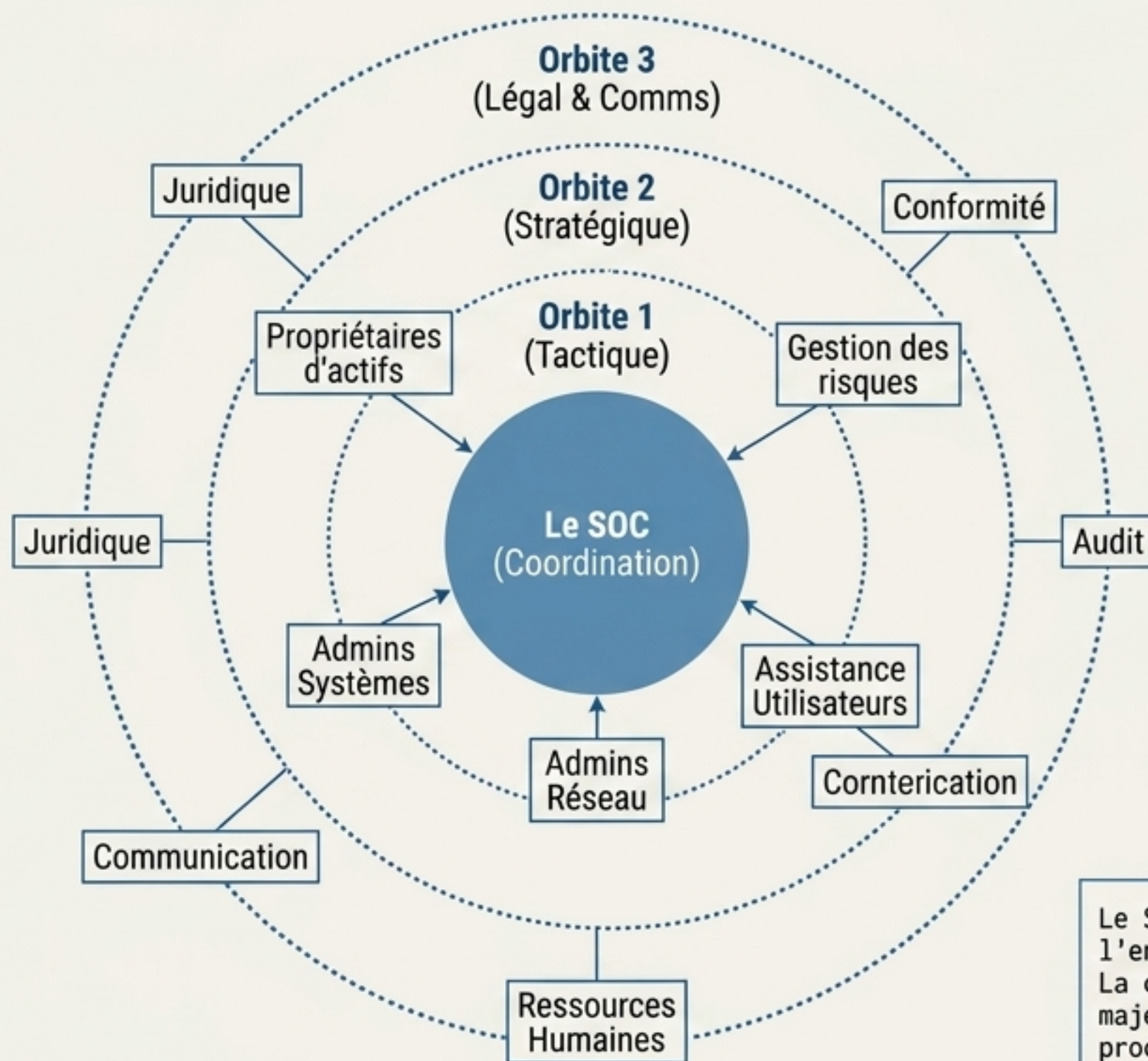
Le piège de la fatigue : Le Gestionnaire d'incidents doit veiller à un déploiement échelonné pour maintenir la lucidité analytique sur la durée de la crise.

Dossier 404

Mobilisation

- Criticité bancaire confirmée.
- Dan réveille Vicki Vale (Gestionnaire d'incidents).
- Vicki centralise la coordination.
- Dan est libéré pour l'analyse forensique réseau experte.

Carte Orbitale de Collaboration Interne



Le SOC ne pilote pas l'entreprise.
La coordination d'un incident majeur bascule vers les processus de crise organisationnels existants.

Dossier 404

Crise et Confinement

- Serveurs virtuels compromis.
- Incident Majeur déclaré par Vicki.
- Dilemme : La déconnexion brutale entraînerait d'énormes pertes financières.
- Décision : Avancer la fenêtre de maintenance pour restaurer silencieusement.

Panneau de Décision Tactique

Data Card

Option A : L'Arrêt Brutal

Éteindre complètement l'ordinateur compromis.

Avantage :
Stoppe l'exfiltration

Inconvénient :
Détruit définitivement les preuves cryptographiques résidant dans la mémoire vive (RAM).

Option B : La Méthode SOC (Sélectionnée)

1. Isoler virtuellement le trafic réseau pour capturer les flux de données (Packet Capture).
2. Mettre la machine en mode 'Hibernation'.

Avantage :
L'hibernation fige l'état de la mémoire vive sur le disque dur, permettant une analyse criminalistique approfondie ultérieure.

Data Card

Dossier 404

Le Poste de Robert

- Désactivation immédiate du compte de Robert.
- Dan isole le réseau local du PC pour analyse des paquets bruts.
- Ordre transmis : Mettre le PC en hibernation.
- Le matériel est saisi physiquement par le SOC.

Spectre des Tiers de Confiance

Data Card

Prestataires (Contractuels)

Périmètre précis,
agissent comme
employés.

Haute flexibilité.

Infrastructure client.

Data Card

Externalisation (Outsourcing)

Service de bout en
bout sur
l'infrastructure client.

Flexibilité moyenne.

SLA définis.

Data Card

Services Gérés (MSSP)

Service complet sur
infrastructure
fournisseur.

Faible flexibilité
(standardisé).

SLA stricts.

Data Card

Motifs de mobilisation

[Surveillance 24/7]

[Renseignement Menaces]

[Intervention d'Urgence]

[Forensique Avancée]

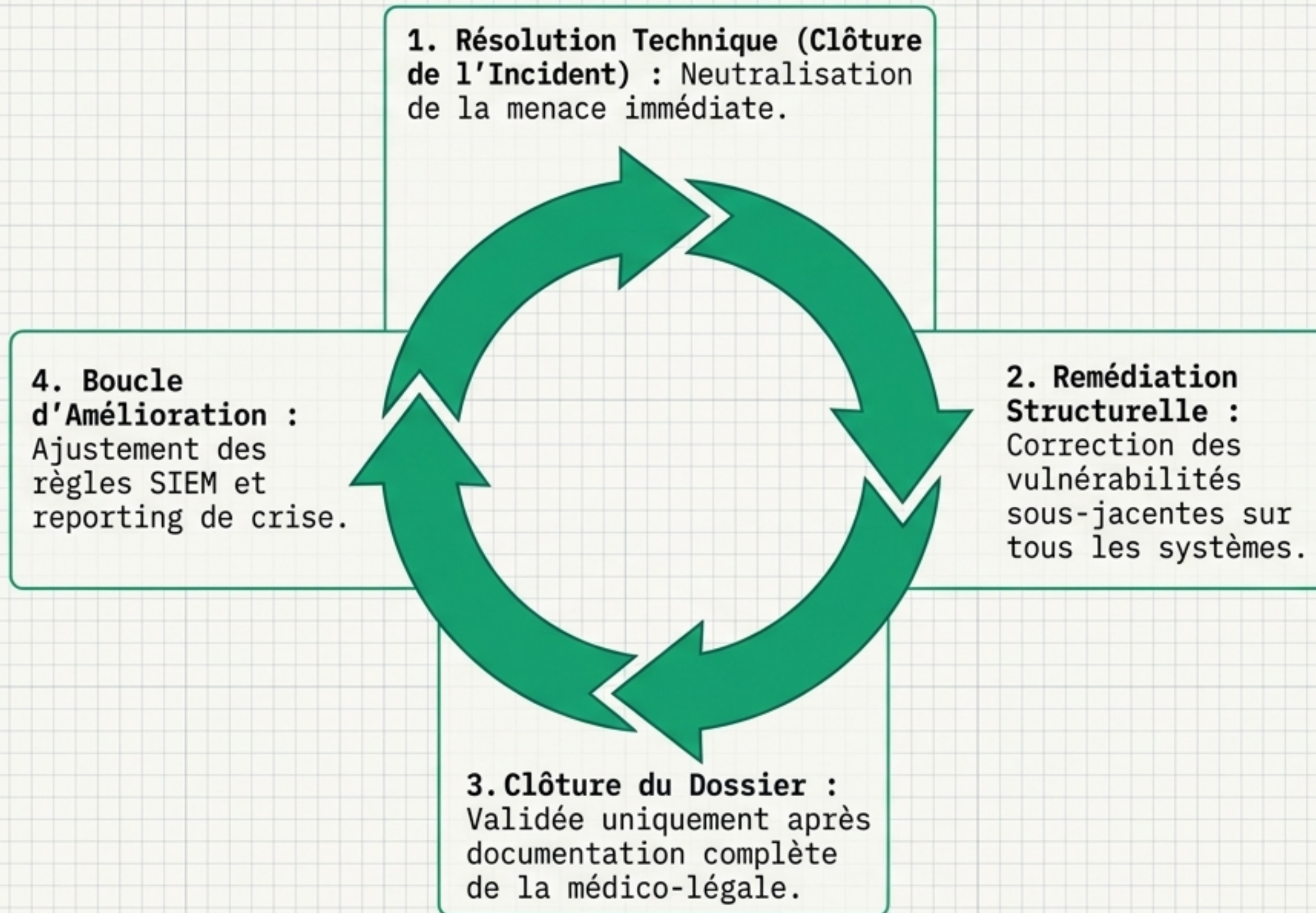
[Renfort Capacité]

Dossier 404

L'Appel aux Tiers

- Renfort de Niveau 1 demandé au prestataire externe.
- Envoi du code malveillant du PC à une firme spécialisée et au fournisseur Antivirus.
- Résultat : Découverte d'un nouveau Cheval de Troie.
- Mise à jour globale de l'antivirus déployée.

La Boucle de Clôture



Dossier 404

Bilan Final

- **Confirmé :** Exfiltration minime (aucune donnée personnelle PII).
- **Vérification :** 3 autres administrateurs ont reçu le courriel mais n'ont pas cliqué.
- **Statut du dossier :** Clos.
- **Condition de clôture respectée :** Correctifs de sécurité appliqués sur l'ensemble de l'architecture pour prévenir toute récurrence.