

DOCUMENT DE
RÉFÉRENCE

Études de cas en criminalistique numérique

Du réseau au terminal

Méthodologies d'investigation appliquées
pour les incidents de sécurité et RH.

CONFIDENTIEL //
RAPPORT D'ENQUÊTE

Les piliers de l'investigation (The Forensic Mindset)

ACTIF #001 : ÉTAT D'ESPRIT



Pilier 1 : Autorité et Impartialité

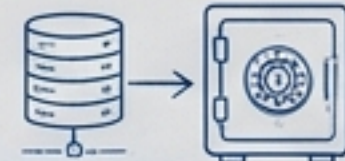
- Déclarer les conflits d'intérêts.
- Valider l'autorisation légale formelle.

Règle d'or : Ne jugez pas la culpabilité, présentez uniquement les faits et les données brutes.



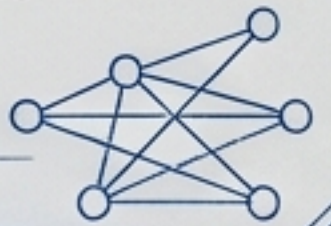
Pilier 2 : Préservation de l'état

- Ne jamais altérer la source originale.
- Système allumé : Conserver les données volatiles.
- Système éteint : Ne pas rallumer sans clonage préalable.



Pilier 3 : Corrélation rigoureuse

- Une seule trace ne suffit jamais.
- L'usurpation d'adresse MAC ou IP est courante.
- Trianguler plusieurs vecteurs de preuves pour établir une vérité indéniable.



Dossier 01 : L'empreinte réseau

DOSSIER 01 : ACTIF

Nature de l'incident : Allégations de harcèlement entre deux employés (Huxley et Sarah).

Mandat des RH : Rassembler les preuves numériques de communication pour appliquer une sanction.

Contraintes de l'enquêteur :

- Isolement total de l'incident.
- Interdiction de qualifier légalement le harcèlement.
- Interdiction d'accéder aux terminaux physiques (recherche réseau uniquement).

Cibles d'acquisition : Journaux Active Directory, proxys web, pare-feux, serveurs de messagerie.

Le triangle de corrélation d'identité

Identity Correlation Triangle

1. L'Authentification (Active Directory)

Événement 4672 : Prouve quelle identité a ouvert une session.

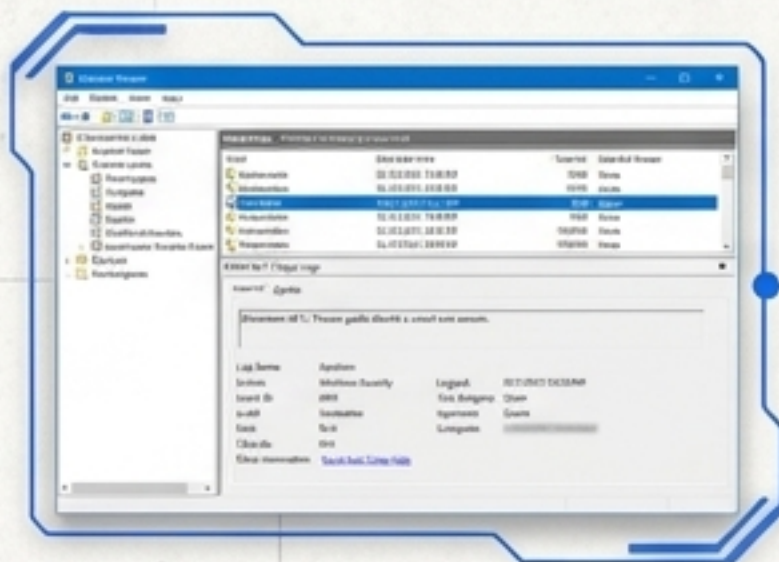
2. L'Empreinte Web (Pare-feu/Proxy)

Cisco Firepower / Squid : Révèle l'activité (ex. réseaux sociaux) depuis une IP.

L'identité est indéniable quand les 3 nœuds s'alignent (IP + Horodatage).

3. L'Intention (Messagerie)

Exchange / Get-MessageTracking : Les signatures numériques lient l'action à l'expéditeur.



Time	Event	Username	Action	Source	Destination	Authentication	IP Address
2017-08-24 14:00:00	User Login	john.doe	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	jane.smith	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	john.doe	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	jane.smith	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	john.doe	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	jane.smith	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	john.doe	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	jane.smith	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	john.doe	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10
2017-08-24 14:00:00	User Login	jane.smith	Success	10.10.10.10	10.10.10.10	Basic Authentication	10.10.10.10



Extraction et vérification des artefacts

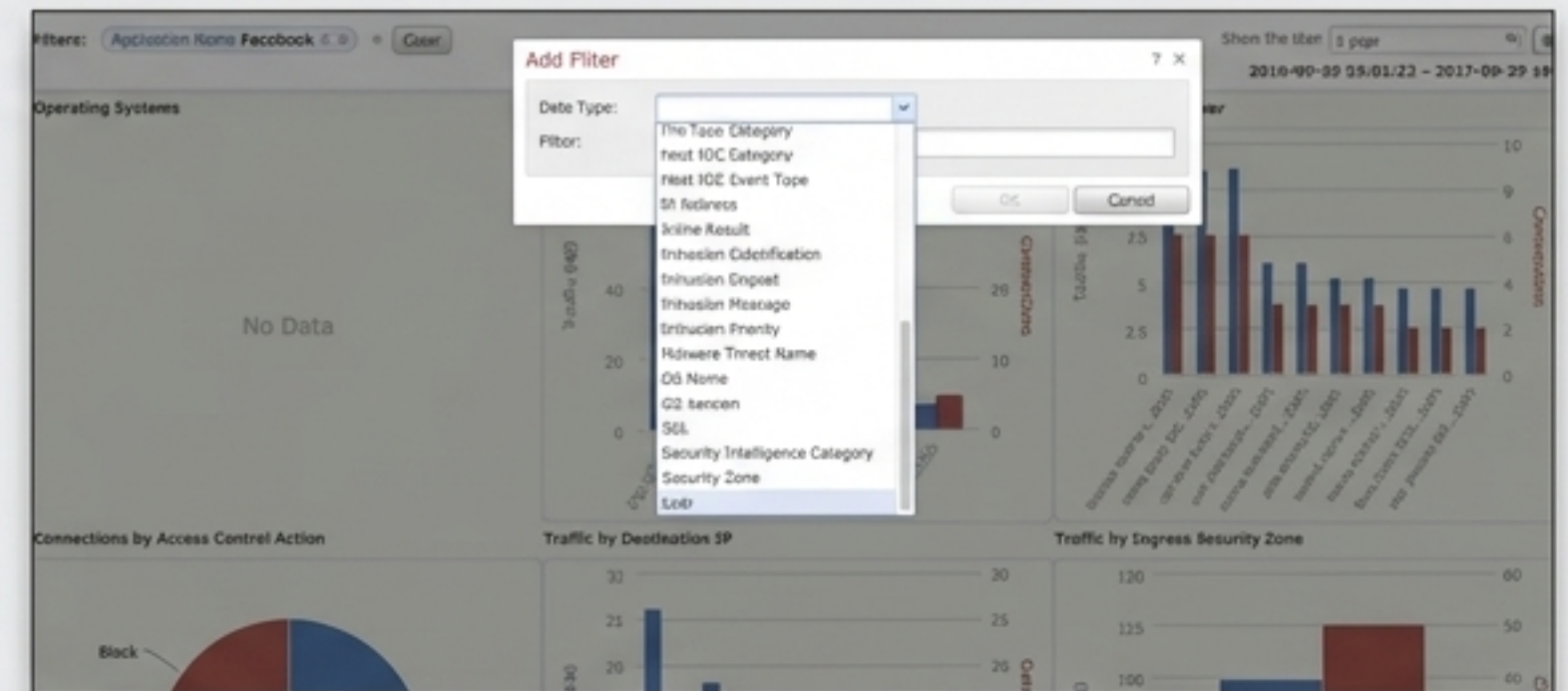
Artefact A : En-têtes SMTP (Falsifiables vs Réels)

- Analyse chronologique inverse requise.
- L'adresse IP la plus ancienne révèle l'origine véritable.
- Horodatage des sauts confirme la validité.

```
Delivered-to: weise968@gmail.com
Received: by 10.28.187.214 with SMTP id 1205csp1378402wsf;
Wed, 11 Oct 2017 18:54:59 -0700 (PDT)
A-Google-Sntp-Source: AunifjCv-ed153374/e/P148SCHC0FPoKgcBcCVVIS5RV4QBvtalh0ddoiLL/GPryl3pMHS6apA
X-Received: by 10.31.179.14 with SMTP id c14mr1268618vbf.167.1507773299866;
ARC-Seal: i=1; a=ssa-sha512; t=1507773299; cn=none;
d=google.com; s=arc-20160816;
b=Vebusv41LRCKkV111NqWhuel135ABBYhPohSe15nx15xPbgBG+tmNeut3bbgCfy+Yu
+OvB1laMBj12nKksod+=638111x7JWoClog=VdVvaBjMN89u/pe221V+OGkgkiglvVgu
xXv6IxK11RGngooBNmSwgfjamd4hr7pc3TvKHDABSiC/FLck0g3sNd8507VhecQv11N0
urzt/UBRX4+YymnRlh/17/musyTVVsuaELDoyBdInjn3nA1lPga21licr6x3ojVRdCV
vFVUXylCJ+OL494e32Vy7VRNaigs8=ReiRuNODoBaa7AHNCSp8olvalah4vQ00QV0Qed
B8nA==
SPF authentication Results: i=1; mx.google.com:
X-Received: by 10.31.179.14 with SMTP id c14mr12686188bvkf.167.1507773299866;
Wed, 11 Oct 2017 18:54:59 -0700 (PDT)
```

Artefact B : Filtrage Contextuel (Firepower)

- Ciblage spécifique des applications (ex. Facebook).
- Période d'analyse ciblée (ex. 12 mois) pour le compte suspect.



ALERTE ROUGE : Les adresses MAC peuvent être usurpées (spoofing). Toujours valider avec l'authentification centralisée ou les historiques cloud (CASB).

L'anatomie du rapport d'expertise

1. Résumé du cas

Les faits initiaux (Qui, quoi, quand). Précision des limites du mandat (ex. "Réseau uniquement").

2. Acquisition

Documentation de la chaîne de possession. Hachage des clés USB, identification des actifs (AD12345, ContentFilter12345) et auditeurs.

3. Constatations (Les Faits)

Indexation des artefacts (ex. Artefacts 8992, 2343). Mention de la validation via des comptes en lecture seule.

4. Conclusion objective

Confirmation d'authenticité : "Nous avons authentifié les communications X et Y."

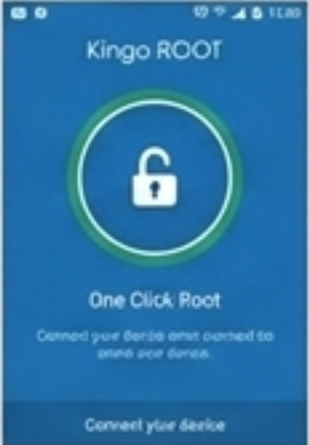
Dossier 02 : La fuite de données (Terminaux)

ESCALATION

- **L'Escalade** : Suite à la notification des RH, le suspect remet sa démission et tente d'effacer des schémas techniques (fichiers JPEG) au profit d'un concurrent.
- **Mandat** : Saisie immédiate de l'ordinateur portable et du téléphone professionnel.
- **Défi légal franchi** : L'employé a préalablement signé une renonciation aux droits de confidentialité (Waiver). Autorisation formelle d'accéder aux systèmes et de contourner les mots
- **Objectif de l'enquêteur** : Clonage physique complet, récupération des données supprimées, et obtention de la preuve d'exfiltration.



Matrice de triage des terminaux (Endpoint Matrix)

Windows (PC Portable)	Android (v5.x)	iOS (iPhone moderne)
Statut : Éteint	Statut : Réinitialisé	Statut : Réinitialisé et chiffré
Action : Ne pas rallumer. Clonage matériel/logiciel à froid (ex. FTK Imager).	Action : Root -> Accès Shell (ADB) -> Montage et Clonage RAW du stockage flash.	Action : Extraction directe impossible sans jailbreak rare.
Recherche : Cible : Exécuter la commande `kind:=picture`.		Stratégie : Alternative : Rechercher une sauvegarde iTunes (chiffrée ou non) sur le PC portable Windows cloné.

L'art de la résurrection des données

ESCALATION

Anatomy of an Exfiltration

T0: Exfiltration

T1: Suppression

**T2: Persistance
silencieuse**

**T3: Résurrection
forensique**

L'utilisateur chiffre et envoie le fichier JPEG original via Outlook à un concurrent.

Suppression du fichier original et vidage de la corbeille. L'index du système est effacé, mais les secteurs RAW restent intacts.

Le fichier système `\AppData\Local\...\Explorer\thumbs.db` conserve silencieusement la miniature et les métadonnées de l'image détruite.

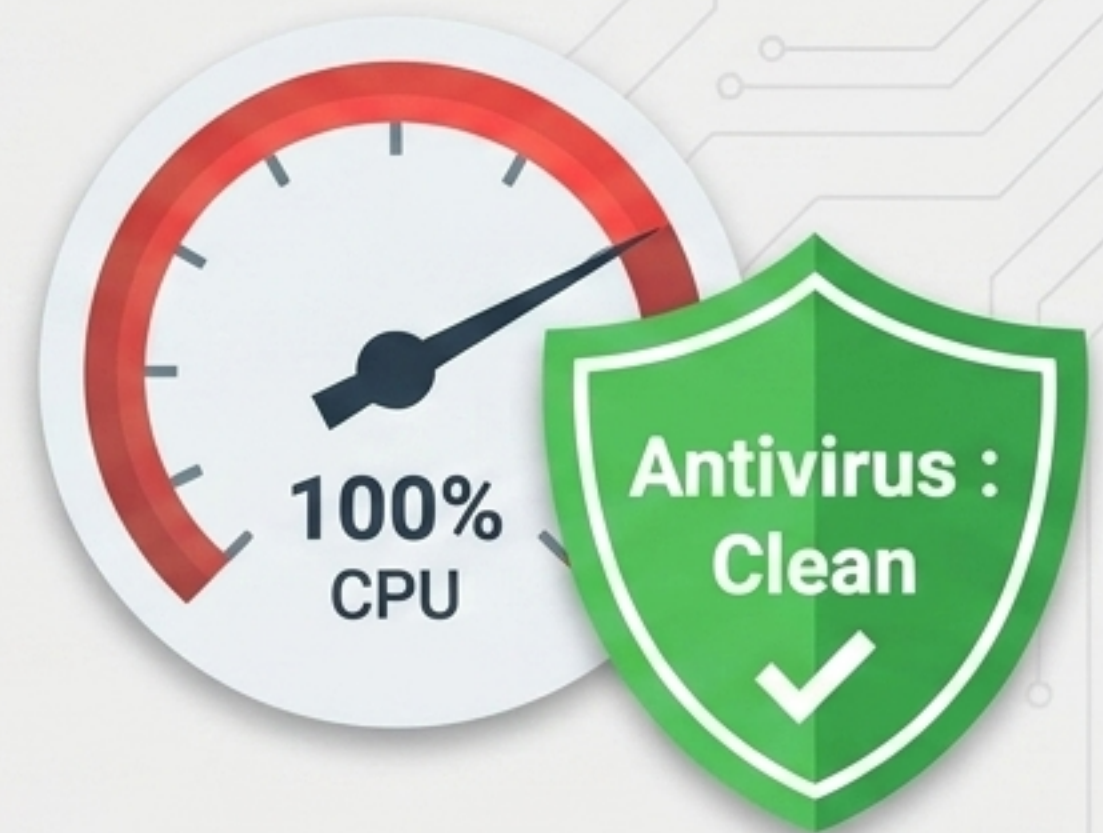
Scan des secteurs RAW ignorant le système de fichiers pour extraire les métadonnées d'origine (date, propriétaire) prouvant la culpabilité.



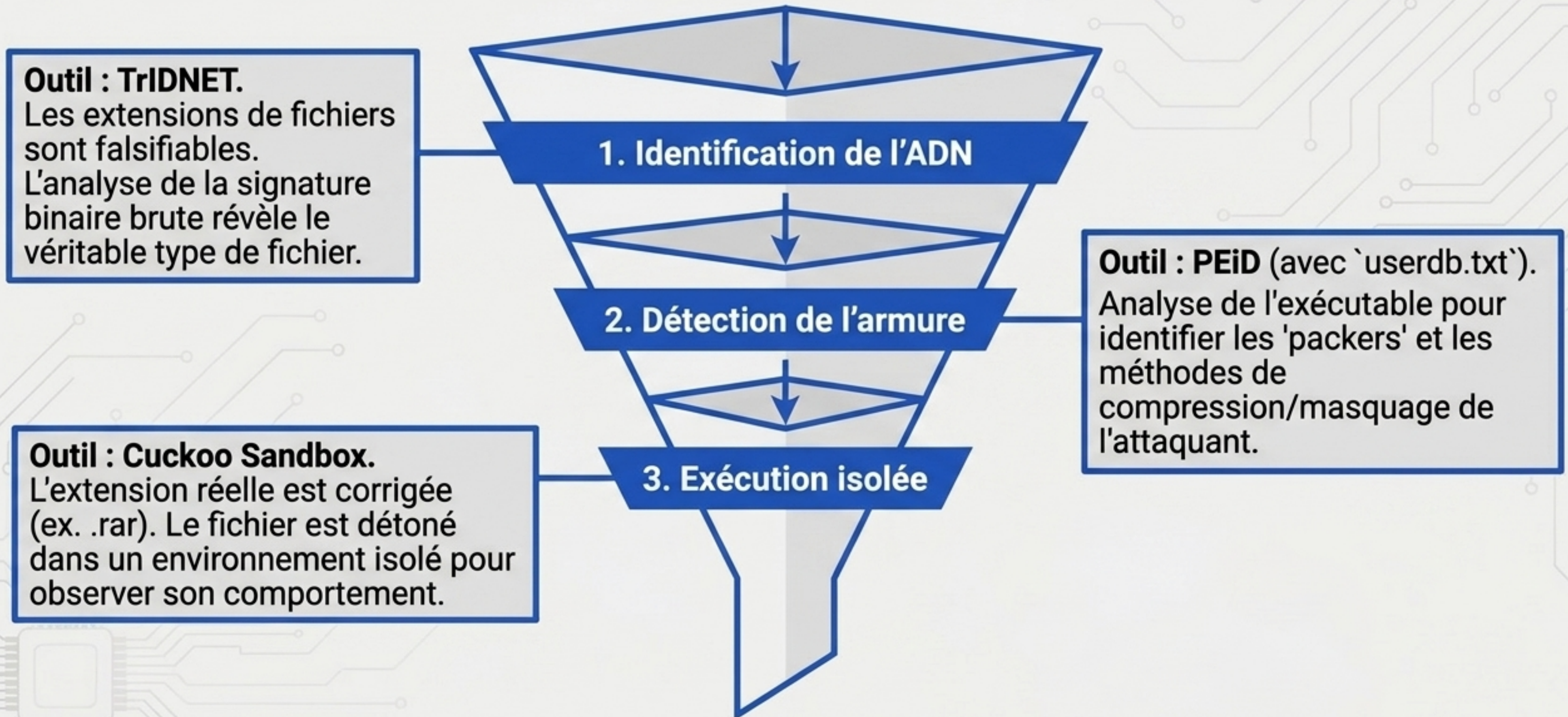
Dossier 03 : La menace silencieuse

ANOMALIE

- **L'Incident :**
Le poste d'un collègue subit une lenteur extrême. Deux processus mystérieux consomment 100% des ressources système.
- **L'Angle mort :**
L'antivirus local et VirusTotal sont complètement aveugles (zéro détection).
- **Le Piège :**
Soumettre le fichier complet à VirusTotal pourrait alerter un attaquant sophistiqué surveillant la plateforme que son outil a été découvert.
- **Mandat :**
Isoler l'anomalie et analyser manuellement et statiquement les processus suspects sans formater immédiatement la machine.



L'entonnoir d'analyse statique



Au-delà de l'infection : La boucle de rétroaction

1. Identifier la charge utile

Comprendre la fonction du malware.

2. Scanner l'hôte

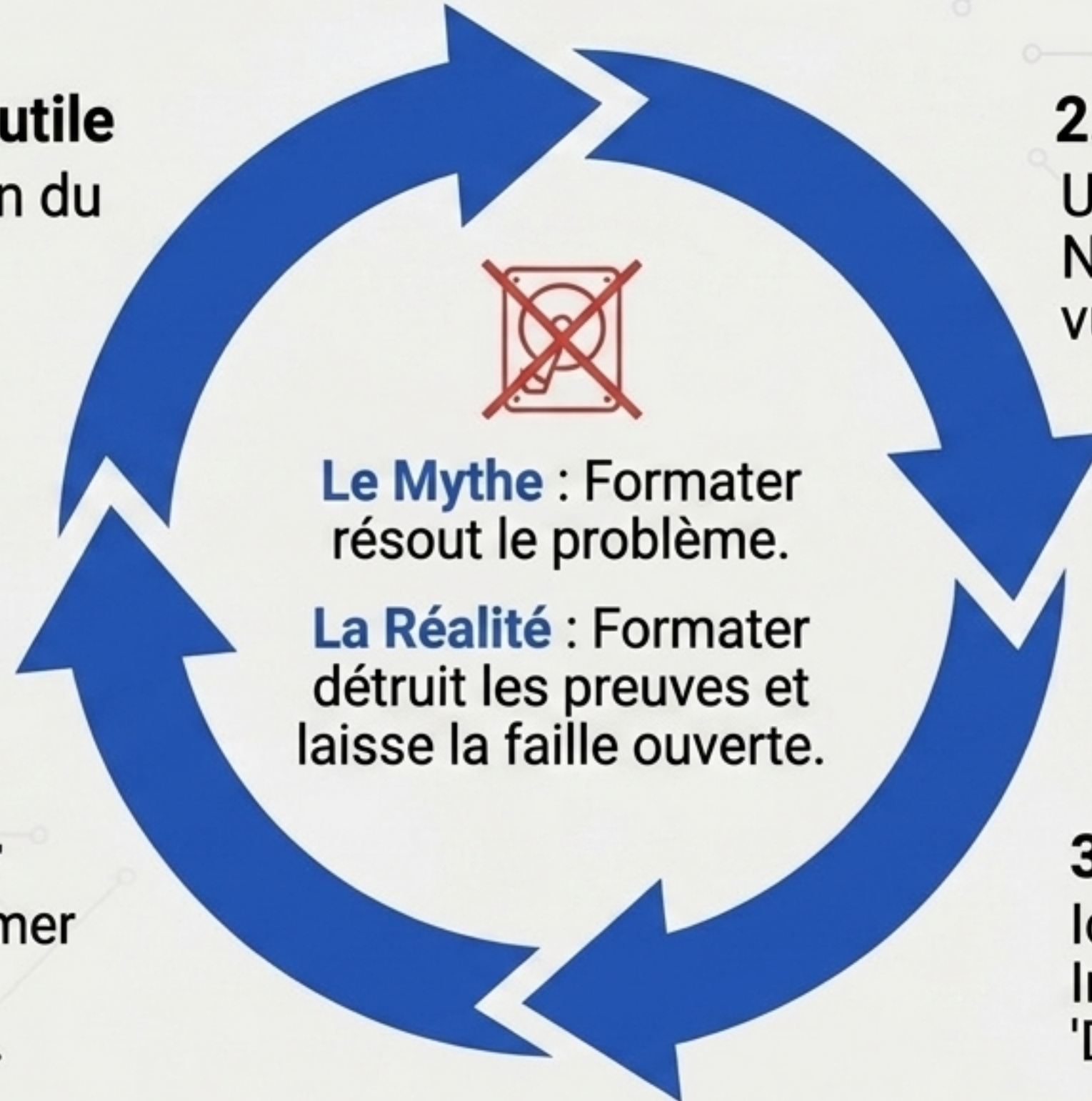
Utiliser OpenVAS ou Nessus pour identifier la vulnérabilité exploitée.

3. Corréler l'utilisateur

Identifier le vecteur (Ex: Installation volontaire de 'DNS Unlocker').

4. Patcher et Former

Corriger la faille et former l'employé avant de reformater le système.



Matrice de la boîte à outils de l'enquêteur



Investigation Réseau

- Cisco Firepower : Filtrage contextuel et réseaux sociaux.
- Squid Proxy : Journaux de filtrage Web.
- PowerShell (Get-MessageTracking) : Logs d'intention Exchange.



Acquisition Terminaux

- Kingo Root : Privilèges et root Android.
- ADB : Accès shell au périphérique.
- FTK Imager / DD : Clonage matériel et extraction RAW.



Récupération de Données

- **PhotoRec** : Récupération RAW des médias et métadonnées.
- **Foremost** : Extraction automatique des fichiers.
- **iPhone Backup Viewer** : Analyse des sauvegardes iTunes.



Analyse de Menaces

- **TrIDNET** : Identification binaire brute.
- **PEiD** : Détection de l'armure et de la compression.
- **Cuckoo Sandbox** : Détonation en environnement isolé.
- **OpenVAS** : Scan de vulnérabilités post-incident.

Le cadre de l'investigation unifiée

1. Vérifier l'autorité

Aucune frappe clavier sans mandat ou renonciation signée.
Élimination formelle des conflits d'intérêts.

2. Préserver l'état

Isoler le réseau ou cloner le matériel.
On n'enquête jamais directement sur le système original en production.

3. Corréler les vecteurs

Ne jamais faire confiance à une seule source.
Croiser continuellement l'IP, le hachage, les logs AD et le proxy.

4. Rapporter sans juger

L'outil technique prouve l'action informatique, les Ressources Humaines ou la justice qualifient l'intention.

L'expérience comble les lacunes

1	• La théorie ne suffit pas	Les environnements réels (chiffrement iOS moderne, architectures cloud) brisent continuellement les approches standards de laboratoire.
2	• Validation continue	Construisez des laboratoires de simulation isolés. Visez les certifications spécialisées (réf: Tom's IT Pro) pour maîtriser l'évolution des menaces.



« Je n'ai pas créé cette situation, je ne fais que la gérer. » — L'état d'esprit ultime de l'enquêteur