PROCÉDURE TECHNIQUE DE GESTION D'INCIDENT CYBER

Objectif : Guider la détection de l'incident jusqu'au retour à la normale, tout en préservant les preuves légales.

PHASE 1 : QUALIFICATION (15 premières minutes)

Dès le signalement par l'utilisateur ou une alerte système.

1. **Vérifier la véracité :** S'assurer qu'il ne s'agit pas d'un faux positif.
2. **Ouvrir une main courante :** Notez **tout** avec l'heure exacte (un simple fichier texte ou un cahier suffit).
    - *Exemple : "14h05 - Appel de M. Dupont. PC lent + icônes bizarres."*
3. **Évaluer la gravité :**
    - *Niveau 1 (Faible)* : Adware, PC isolé, pas de données sensibles.
    - *Niveau 2 (Moyen)* : Compte administrateur compromis, virus sur un serveur non critique.
    - *Niveau 3 (Critique)* : Ransomware, fuite de données, Contrôleur de Domaine touché.

PHASE 2 : CONFINEMENT

Priorité absolue : Empêcher la propagation au reste du réseau (VLANs, VPN, DMZ).

A. Confinement Réseau (Isoler sans éteindre)

Le but est de couper l'attaquant sans perdre les données en RAM (mémoire vive).

1. **Déconnecter la machine infectée du réseau :**
    - Débrancher le câble RJ45 physiquement.
    - OU couper le port sur le switch (via CLI : `shutdown` sur l'interface correspondante `eX/Y`).
    - OU couper le Wi-Fi sur l'appareil.
2. **Si l'attaque vient du VPN :**
    - Tuer la session VPN sur le Firewall A (`kill user` ou désactiver le compte VPN).
    - Bloquer l'IP source dans une règle "DENY" temporaire tout en haut des règles du Firewall.

3. **Si c'est un Ransomware avéré (propagation rapide) :**
    - N'hésitez pas à isoler le VLAN complet (ex: VLAN 10 Compta) en coupant l'interface virtuelle sur le routeur/cœur de réseau.

B. Confinement Identité

1. **Réinitialiser le mot de passe** de l'utilisateur compromis (AD).
2. **IMPORTANT :** Si vous suspectez que l'attaquant a volé des identifiants Admins, changez **immédiatement** le mot de passe du compte `krbtgt` (Kerberos) et des administrateurs du domaine.

PHASE 3 : ANALYSE & FORENSIQUE

Ne touchez à rien sur le disque avant cette étape si vous voulez des preuves.

1. **Dump de la RAM :** Si le PC est encore allumé, utilisez un outil sur clé USB (ex: *FTK Imager Portable*) pour copier la RAM. C'est là que résident les clés de chiffrement et les mots de passe.
2. **Copie du Disque :** Idéalement, clonez le disque dur (copie bit-à-bit) avant d'essayer de nettoyer. Copiez la copie du disque afin de travailler sur la 2e copie, jamais sur l'original ni sur la 1ère copie.
3. **Identifier le "Patient Zéro" :**
    - Regardez les logs Firewall : Vers quelle IP externe le malware essaie-t-il de communiquer (C&C) ?
    - Regardez les logs Proxy/DNS : Quel domaine a été requêté ?

PHASE 4 : ÉRADICATION

Ne faites pas confiance à un antivirus pour "nettoyer" un PC compromis en profondeur.

1. **Tout effacer et reconstruire.**
    - Formatez complètement le disque dur.
    - Réinstallez l'OS depuis une image saine (Master).
2. **Traitement de la faille :**
    - Si le malware est entré par une faille Windows -> Appliquez le correctif (KB) manquant sur **tout** le parc avant de reconnecter le PC.
    - Si c'est par RDP/SSH -> Vérifiez vos règles Firewall.

PHASE 5 : RÉCUPÉRATION

1. **Restauration des données :**
    - Restaurer depuis une sauvegarde **froide** (hors ligne) ou immuable.
    - **ATTENTION :** Scannez la sauvegarde avant de la restaurer. Il arrive que les hackers infectent les sauvegardes 2 semaines avant de déclencher l'attaque. Remontez assez loin dans le temps si ce n'est pas une sauvegarde immuable.
2. **Surveillance accrue :**
    - Une fois le PC reconnecté, placez une vigilance accrue sur les logs réseau pendant 48h.

PHASE 6 : OBLIGATIONS LÉGALES

1. **Notification CNIL (RGPD) :**
    - Si des données personnelles (noms, emails, salaires, numéros sécu...) ont été potentiellement volées ou chiffrées : Vous avez **72 heures** maximum pour déclarer l'incident sur le site de la CNIL.
2. **Dépôt de plainte :** Recommandé pour les assurances cyber (gendarmerie ou police).
3. **Rapport d'incident :** Rédigez un document expliquant :
    - Ce qui s'est passé.
    - Pourquoi c'est arrivé (la faille).
    - Ce que vous avez fait pour que ça ne recommence plus.