

Module 03

Cybersecurity 3

Rapport d'Investigation Forensique

1. Informations Générales

- **Titre du rapport :**
 - **Référence du dossier :**
 - **Nom de l'enquêteur :**
 - **Organisation / Service :**
 - **Date de début de l'investigation :**
 - **Date de fin de l'investigation :**
 - **Version du rapport :**
 - **Classification** (ex : Confidentiel, Diffusion restreinte) :
 - **Audience cible** (ex : Responsable SSI, Équipe juridique, Direction générale) :
-

2. Contexte de l'Investigation

Fournir un résumé du contexte qui a déclenché l'investigation (alerte SOC, incident signalé, audit, plainte, etc.)

- **Origine de l'alerte ou de la demande :**
 - **Date et heure de l'incident présumé :**
 - **Description succincte de l'incident :**
 - **Périmètre analysé** (poste utilisateur, serveur, réseau, etc.) :
-

3. Objectifs de l'Investigation

Décrire les objectifs de la mission d'analyse forensique.

- **Déterminer si une compromission a eu lieu**



- Identifier les vecteurs d'attaque
- Évaluer l'étendue de l'incident
- Identifier les données impactées
- Collecter les éléments de preuve
- Émettre des recommandations correctives

4. Chronologie des Événements (Timeline)

Date / Heure (UTC) Événement Source Commentaire

5. Méthodologie

Détailler la démarche utilisée, en se référant à un standard si pertinent (ISO 27037, NIST SP 800-86, etc.)

- **Préservation des preuves :**
 - **Acquisition** (type de données collectées, outils utilisés, formats, hash MD5/SHA256) :
 - **Analyse** (techniques et outils utilisés : Autopsy, FTK, Volatility, etc.) :
 - **Documentation et chaînage de preuve** (chain of custody) :
-

6. Éléments Collectés

Type de Donnée	Nom / Chemin	Méthode d'Acquisition	Hash MD5 / SHA256	Remarques
----------------	--------------	-----------------------	-------------------	-----------

7. Résultats de l'Analyse

Détaillez ici ce que vous avez observé pendant l'analyse.

7.1 Indicateurs de compromission (IOC)

- IP malveillantes :
- Fichiers suspects :
- Hashs malveillants :



- Comportements anormaux :
- Processus ou services suspects :
- Modifications de registres / configurations :

7.2 Analyse des artefacts système

- **Prefetch :**
- **Fichiers LNK :**
- **Registre** (Run keys, UserAssist, etc.) :
- **Historique de navigation :**
- **Journaux d'événements (EVTX) :**

7.3 Analyse réseau (si applicable)

- **PCAP / Netflow / journaux de pare-feu :**
- **Connexions anormales :**
- **Tunnels chiffrés, exfiltration suspecte :**

7.4 Analyse mémoire (si applicable)

- **Processus actifs :**
- **DLL injectées :**
- **Clés ou données en clair :**

8. Conclusion de l'Investigation

Résumer les conclusions majeures :

- **Nature de l'incident :** (ex : ransomware, vol de données, compromission d'un compte, etc.)
 - **Origine probable :**
 - **Durée estimée de la compromission :**
 - **Impact constaté / estimé :**
 - **Preuves formelles :**
 - **Attribution (si possible) :**
-

9. Recommandations

Fournir des actions préventives ou correctives

- Mesures de remédiation immédiate
 - Renforcement de la sécurité des systèmes impactés
 - Surveillance accrue / mise en place de détections
 - Mise à jour des antivirus / EDR
 - Formation ou sensibilisation des utilisateurs
 - Réévaluation des politiques de sécurité
-

10. Annexes

- Captures d'écran
- Commandes utilisées
- Résultats d'outils
- Logs horodatés
- Copies des artefacts (si autorisé)