TE RAMA

CSIRT-TERAMA

Incident Cyber : Méthode et outils pour préserver une scène de cybercrime

Rédacteur	Jérémy MOUNIER
TLP	TLP:GREEN
Version	1.0

02/07/2024

Agenda

TLP:GREEN

- Introduction et méthodologies
- Première réponse, les bons reflexes
- Focus sur DFIR-ORC

/whoami

Sortie d’école informatique en 2009

Co-fondateur de ArxSys et DFF, logiciel libre d’investigation numérique jusqu’en 2015

Depuis 2015, **Analyste CSIRT et consultant cybersécurité opérationnelle**

~~Obligations~~ Cadre réglementaire

TLP:GREEN

TE RAMA

Depuis 2004 avec la norme PCI-DSS plusieurs règlementations sont venues définir les pratiques en matière de **gestion et de notification des incidents cyber**

…

Prochainement la NIS2 viendra élargir le périmètre des organisations concernées

- *Norme PCI-DSS*
- *Loi Programmation Militaire*
- *RGPD*
- *NIS2*

Référentiels de gestion des incidents cyber

Principaux référentiels proposés pour la **gestion des incidents cyber**

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

ISO
International Organization for Standardization

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

SANS

- **ISO 27035**
- **NIST SP 800-61 rev2**
- **Model PICERL**
- **Referentiel PRIS**
- **Guides ENISA**

…

R&ACT Framework

- https://atc-project.github.io/atc-react/
- Même philosophie que le framework ATT&CK®
- Basé sur la méthodologie PICERL du SANS
- Cas d’usages principaux
  - Outils pour réaliser un « gap analysis »
  - Aide à la construction de playbook et fiches reflexes

Méthodologie

ISO
International
Organization for
Standardization

ANSSI

NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

SANS

- Préparation
- Détection & signalement
- Analyse & endiguement
- Éradication & remédiation
- Apprentissage

Méthodologie

International Organization for Standardization

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

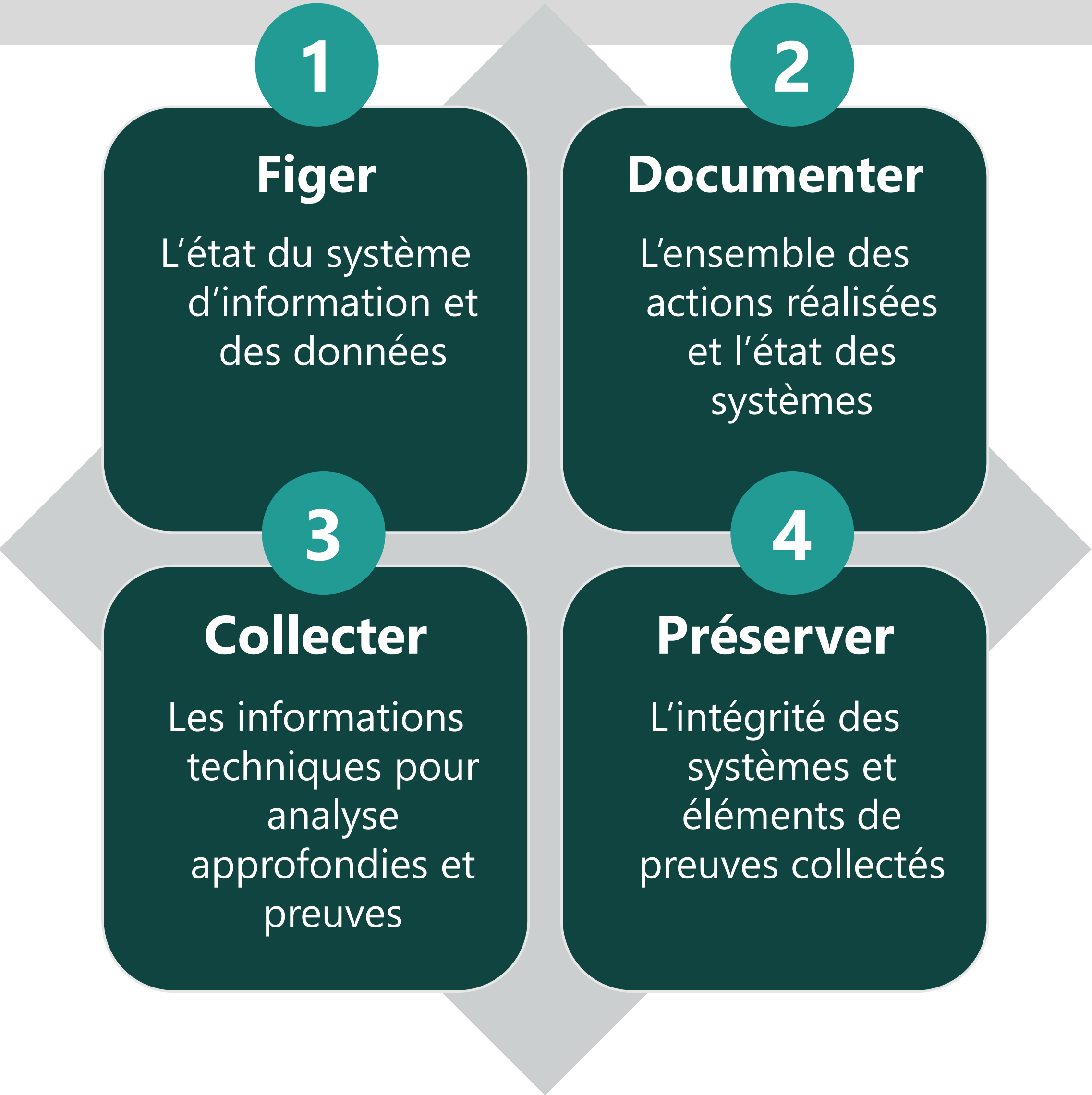
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

SANS

!! PREMIERE REPONSE !!

- Préparation
- Détection & signalement
- Analyse & endiguement
- Éradication & remédiation
- Apprentissage

Première réponse



1
Figer
L'état du système d'information et des données

2
Documenter
L'ensemble des actions réalisées et l'état des systèmes

3
Collecter
Les informations techniques pour analyse approfondies et preuves

4
Préserver
L'intégrité des systèmes et éléments de preuves collectés

Les 4 règles d'or pour préserver une scène de cybercrime

Première réponse

L'utilisateurs, le premier maillon de la chaîne de preuve

1. Arrêter immédiatement toute actions sur le système
2. Signaler le plus rapidement possible l'évènement
3. Horodater et consigner l'ensemble des actions réalisées
4. Prendre des captures d'écrans / photographies

Equipes IT / sécurité / infra, les premiers secours

1. Enregistrer et consigner l'évènement dans le système (ITSM, etc) avec une chronologie détaillée
2. Identifier les premiers impacts (données, infrastructure)
3. Signaler aux équipes sécurité (RSSI, etc.)
4. Sécurisé le périmètre (premières actions d'endiguements)
5. **Collecter les premiers éléments techniques**

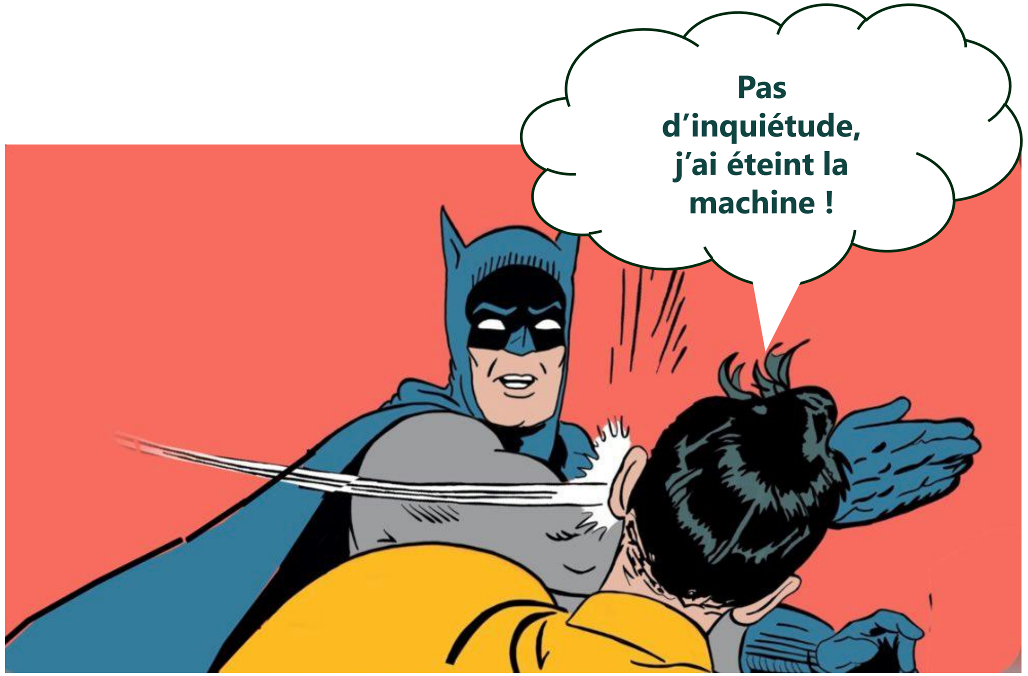
Première réponse

Redevenir opérationnel ASAP, une fausse bonne idée

- Eteindre la machines
- Réinstaller les systèmes
- Restauration rapide des sauvegardes
- Analyses AV
- Réaliser des recherches / analyses depuis le poste victime
- Appliquer les MAJ

→

Pollution des systèmes
Perte de données potentielles
Création de « bruits de fonds »



Préserver la preuve : Cas des systèmes « lives »

- Collecter / analyser les données qui seront perdues une fois le système éteint
- Limiter au maximum les interactions directes avec le système (branchement de périphériques, recherches, etc.)
- Utiliser des logiciels de collecte ou d'analyse intégrants des fonctions de blocage en écriture logiques (drivers en lecture seuls)

Données d'interets

- Les processus en cours d'exécution
- Les communications réseaux
- Les sessions utilisateurs
- Journaux d'évènements / fichiers temporaires
- L'ensemble des données présentes dans la mémoire vive
- Etc.

Stratégie et périmètre de collecte

Investigation d’un système « vivant »

Investigation Post-mortem

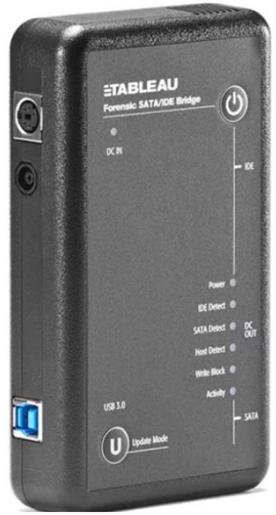
Investigation numérique sur Périmètre Restreint

Investigation numérique sur Large Périmètre

- **Serveurs d’infrastructure système**
  - Authentification, télédistribution, télégestion et prise de main à distance, sauvegarde, supervision, virtualisation, serveurs de fichiers, etc.) ;
- **Serveurs d’infrastructure réseau**
  - Serveurs mandataire, serveurs DNS, etc.;
- **Equipements d’infrastructure réseau**
  - Concentrateur, routeur, point d’accès sans fil, ..
- **Equipements de sécurité**
  - Pare-feu, antivirus / EDR, chiffreurs, … ;
- **Postes d’administration et postes utilisateur**
  - Windows, Mac Linux, etc.
- **Serveurs métier**
  - Serveurs Web, base de données, etc.

Assurer la chaine de preuve

- Bloqueurs en écriture physiques
- Utiliser des logiciels spécialisés pour la collecte et l'analyse
  - Open Source (DD, Guymager, Autopsy, etc.)
  - Commerciaux (Encase, FTK, Magnet Forensics, Xways, etc.)
- Utilisation des formats forensics standards
  - EWF, RAW, AFF, etc.
- Calcul des empreintes cryptographiques à chaque étapes
- Conserver sous clé l'ensemble des éléments de preuves ou supports d'éléments de preuves



Boîte à outils

Côté matériels	Côté logiciels
✓ XX Clés USB vierges (beaucoup) ✓ 2 disques USB de grande capacité ✓ 1 bloqueur en écriture matériel ✓ Une machine d'analyse portable ✓ Des câbles de toute sortes (alimentation, USB, etc.) ✓ Un appareil photo Papier / stylos	✓ Distribution linux d'investigation fonctionnelle et à jour (KALI, SIFT, DEFT, TSURUGI, Home made) ✓ Logiciel d'acquisition de support de stockages (DD, Guymager, FTK Imager, etc.) ✓ Logiciel d'acquisition de la mémoire vive (Winpmem, dumpIT) ✓ Logiciel de collecte systèmes (DFIR-ORC) ✓ Logiciels d'analyses (Autopsy, Photorec, DFF, Volatility, etc.)

DFIR-ORC

DFIR (Digital Forensics & Incident Response) - **ORC** (Outils de Recherche de Compromission)

- **Outil créé et publié par l’ANSSI**
- **Interne depuis 2011 et Open Source depuis 2019**
- **https://dfir-orc.github.io/**
- **Mécanisme intégré de préservation du système**

“One Binary to Run Them All”

DFIR ORC
ANSSI

1

La copie sélective d'artefacts sur tout ou une partie du système d'information dans le cadre d'une réponse à incident.

L'objectif est de « figer la scène » suite à une compromission afin de pouvoir effectuer les analyses et remonter la chaîne de compromission.

2

La recherche d'indicateurs de compromissions et de menaces (Threat Hunting) sur tout ou une partie du système d'information.

ORC permet la collecte à grande échelle d’artefacts ciblés afin de rechercher des techniques ou des modes opératoires qui auront été définis au préalable.

DFIR-ORC : Commandes intégrés

TLP:GREEN

```
C:\> DFIR-ORC_x64.exe <commande> <paramètres>
```

Commande	Fonction
FatInfo	collecte les métadonnées FAT du système de fichiers
FastFind	Recherche des indicateurs système (fichiers, clés de registre, objets Windows type mutex, etc.) spécifiés au sein d'un fichier de configuration XML. Cette commande permet également l'usage de règles Yara
GetSamples	Automatise la collecte d'artefacts potentiellement malveillants, souvent nécessaires a posteriori dans le cadre des analyses comme les binaires s'exécutant au démarrage, les binaires, pilotes et bibliothèques chargées associées aux processus en cours, etc.
GetSectors	Collecte les secteurs du disque contenant les codes d'amorçage et les secteurs non partitionnés
GetThis	Collecte de fichiers sur un système de fichiers NTFS en s'appuyant sur des recherches avancées (regex, chemin, hash, ADS, attributs étendus, règles YARA, etc.) ;
NTFSInfo	collecte les métadonnées NTFS (fichiers, timestamps, empreintes, etc.) ;
NTFSUtil	Outil bas niveau permettant l'inspection de la MFT
ObjInfo	collecte les objets nommés de Windows (canaux nommés, mutex, etc.) ;
RegInfo	collecte les informations présentes dans les bases de registre ;
USNInfo	collecte le journal USN.
ToolEmbed	Permet de générer un binaire de collecte (ORC configuré)

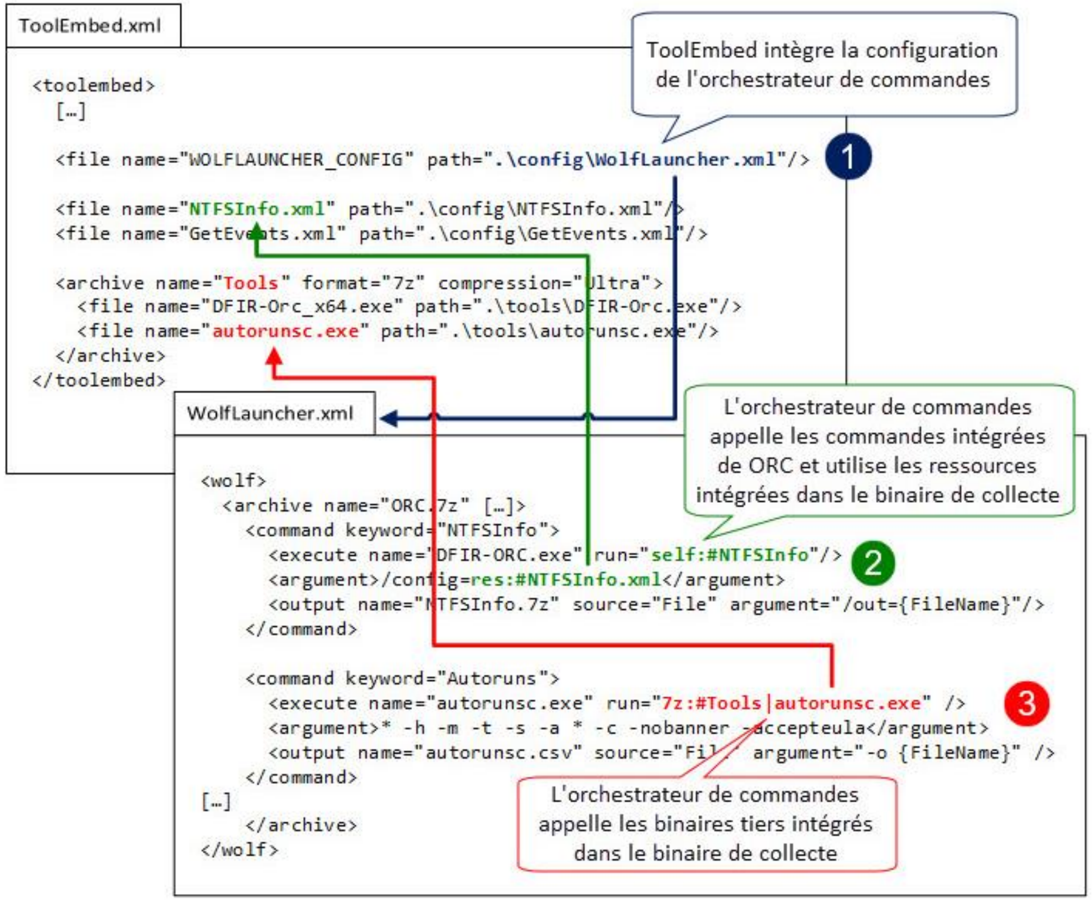
```
C:\> DFIR-ORC_x64.exe GetThis /?
```

ORC Configuré Vs Non Configuré

DFIR (Digital Forensics & Incident Response) - **ORC** (Outils de Recherche de Compromission)

ORC
non
configuré

ORC
Configuré



ToolEmbed intègre la configuration de l'orchestrateur de commandes

```
<toolembed>
  [...]

  <file name="WOLFLAUNCHER_CONFIG" path=".\config\WolfLauncher.xml"/>

  <file name="NTFSInfo.xml" path=".\config\NTFSInfo.xml"/>
  <file name="GetEvents.xml" path=".\config\GetEvents.xml"/>

  <archive name="Tools" format="7z" compression="Ultra">
    <file name="DFIR-Orc_x64.exe" path=".\tools\DFIR-Orc.exe"/>
    <file name="autorunsc.exe" path=".\tools\autorunsc.exe"/>
  </archive>
</toolembed>
```

L'orchestrateur de commandes appelle les commandes intégrées de ORC et utilise les ressources intégrées dans le binaire de collecte

```
<wolf>
  <archive name="ORC.7z" [...]>
    <command keyword="NTFSInfo">
      <execute name="DFIR-ORC.exe" run="self:#NTFSInfo"/>
      <argument>/config=res:#NTFSInfo.xml</argument>
      <output name="NTFSInfo.7z" source="File" argument="/out={FileName}"/>
    </command>

    <command keyword="Autoruns">
      <execute name="autorunsc.exe" run="7z:#Tools|autorunsc.exe" />
      <argument>* -h -m -t -s -a * -c -nobanner -accepteula</argument>
      <output name="autorunsc.csv" source="File" argument="-o {FileName}" />
    </command>
[...]
    </archive>
</wolf>
```

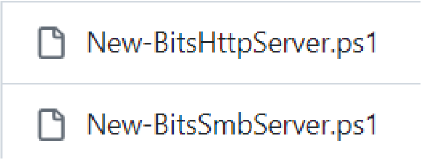
L'orchestrateur de commandes appelle les binaires tiers intégrés dans le binaire de collecte

DFIR ORC
ANSSI

Méthodes de déploiement

DFIR (Digital Forensics & Incident Response) - **ORC** (Outils de Recherche de Compromission)

- > Déploiement au cas par cas sur une machine
  - Manuel via clé USB ou script
- > Déploiement décentralisé
  - Utilisation d'un serveur pour réceptionner les artefacts


New-BitsHttpServer.ps1
New-BitsSmbServer.ps1

Pour aller plus loin

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

AD TIMELINE

DFIR ORC
ANSSI

DFIR4vSphere

Nous contacter

✉ CSIRT @ TERAMA . PF

CSIRT
TE RAMA

- Fingerprint : 287E CCC6 3E31 93EF EE15 0CFE 70CD 0ABD BCFF EC3C
- Key ID : 0x70CD0ABDBCFFEC3C
- Expire : 30/01/2027
- User ID : CSIRT-TERAMA
- Public Key : https://github.com/CSIRT-TERAMA/ressources/