MÉTHODOLOGIE D'UNE ATTAQUE PAR

RANÇONGICIEL

Caillet Evan
Blois Arthur
Dandre Alexis

15/10/2024

Définitions :

Méthodologie : *Ensemble de techniques*

+

Attaque : *Action offensive*

Cyberattaque : *Attaque visant un système informatique*

Rançongiciel : *Logiciel malveillant chiffrant données*

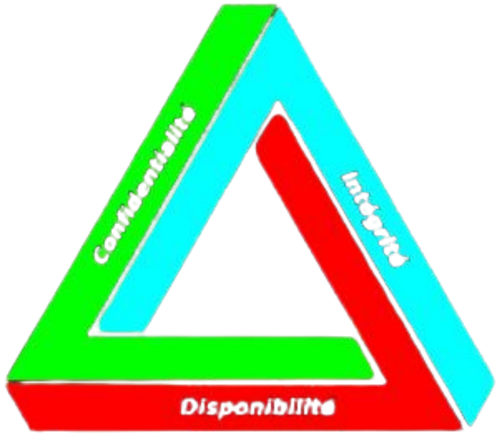
Problématique :

Comment se déroule une attaque par rançongiciel et comment se préparer à une éventuelle attaque ?

Plan :

I. Procédés de l’attaque

II. Comment se protéger



Source : cnil.fr, paperblog.fr

I. Procédés de l’attaque

I.I Reconnaissance

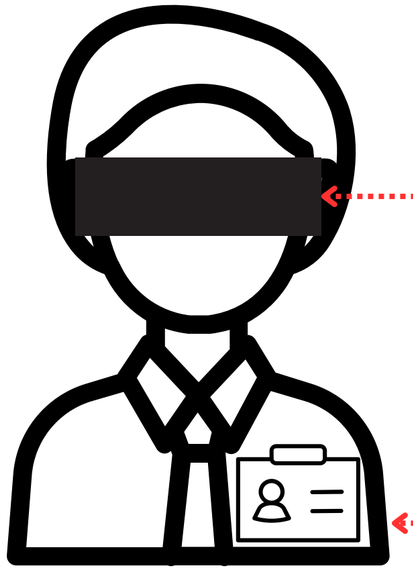
I.II Intrusion et Persistance

I.III Élévations des privilèges et actions

I. Procédés de l’attaque

I.I Reconnaissance

Reconnaissance passive



Recherche sur internet

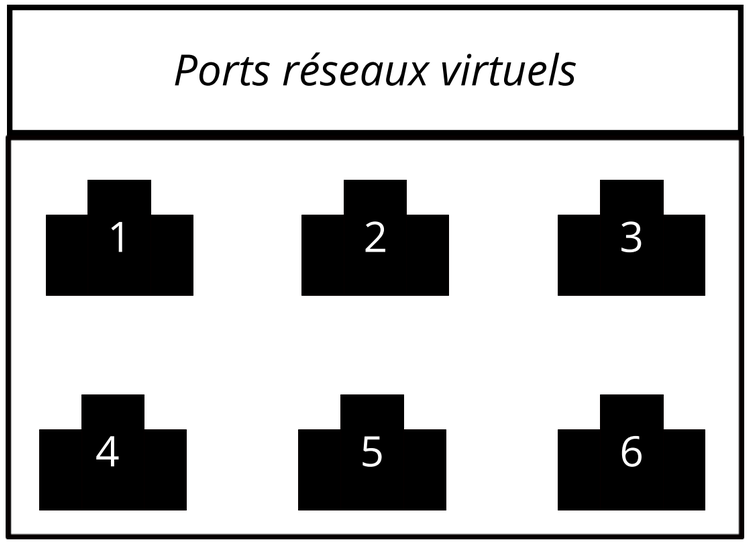
Nom, statut, entreprise

Outils de reconnaissance :
Réseaux sociaux
Noms de domaine
Google Hacking

I. Procédés de l’attaque

I.I Reconnaissance

Reconnaissance active



Analyse du système :

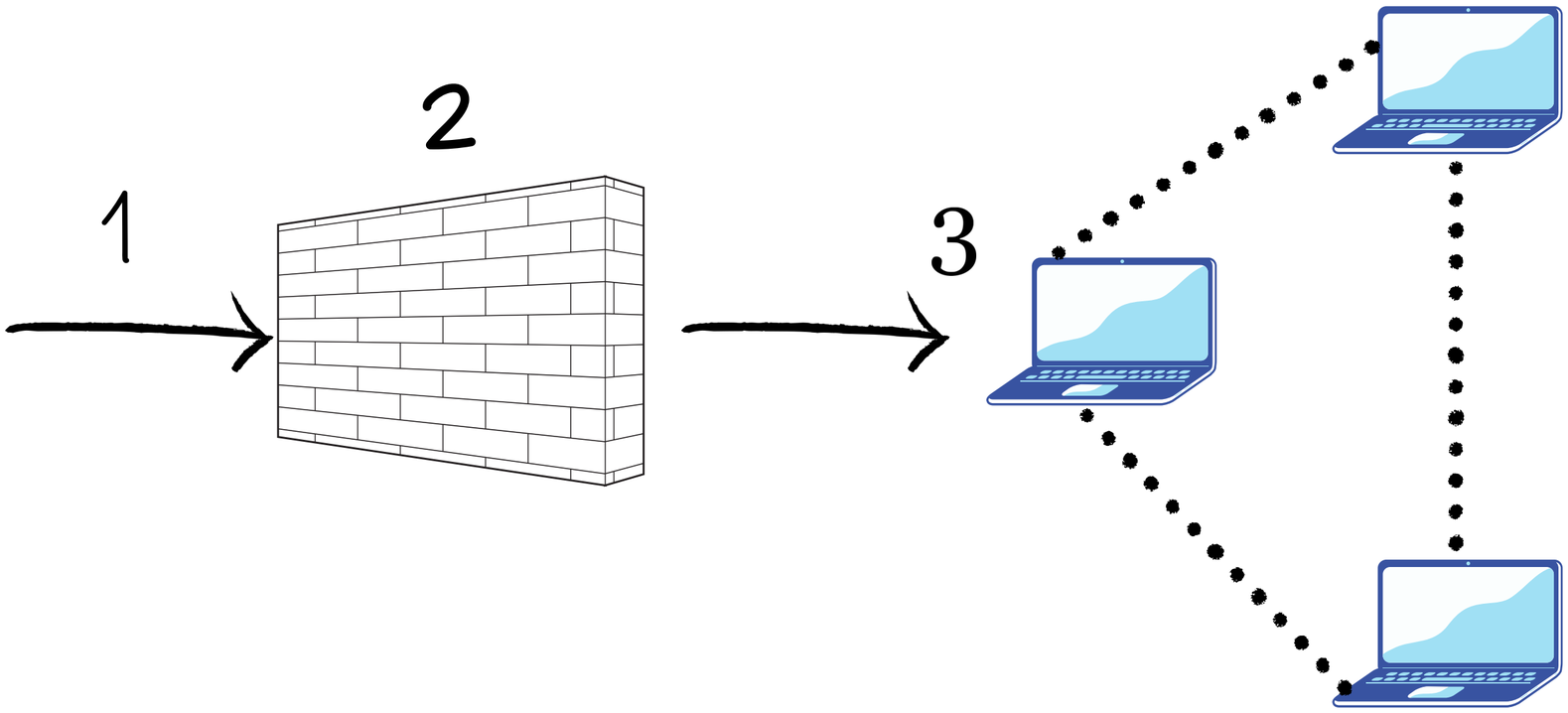
Amorce avec hameçonnage

Détection de failles (ex : ports)

I. Procédés de l’attaque

I.II Intrusion et Pérsistance

Intrusion

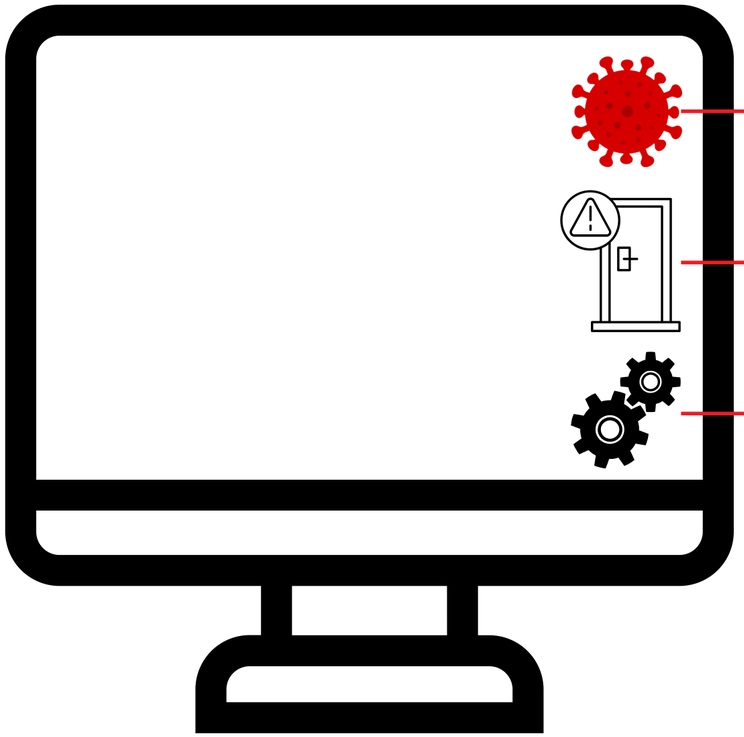


Procédés :
1) Tentative accès
2)Exploitation failles (phishing, Zero Days, ingénierie sociale)
3)Accès à un poste du réseau

I. Procédés de l’attaque

I.II Intrusion et Pérsistance

Pérsistance

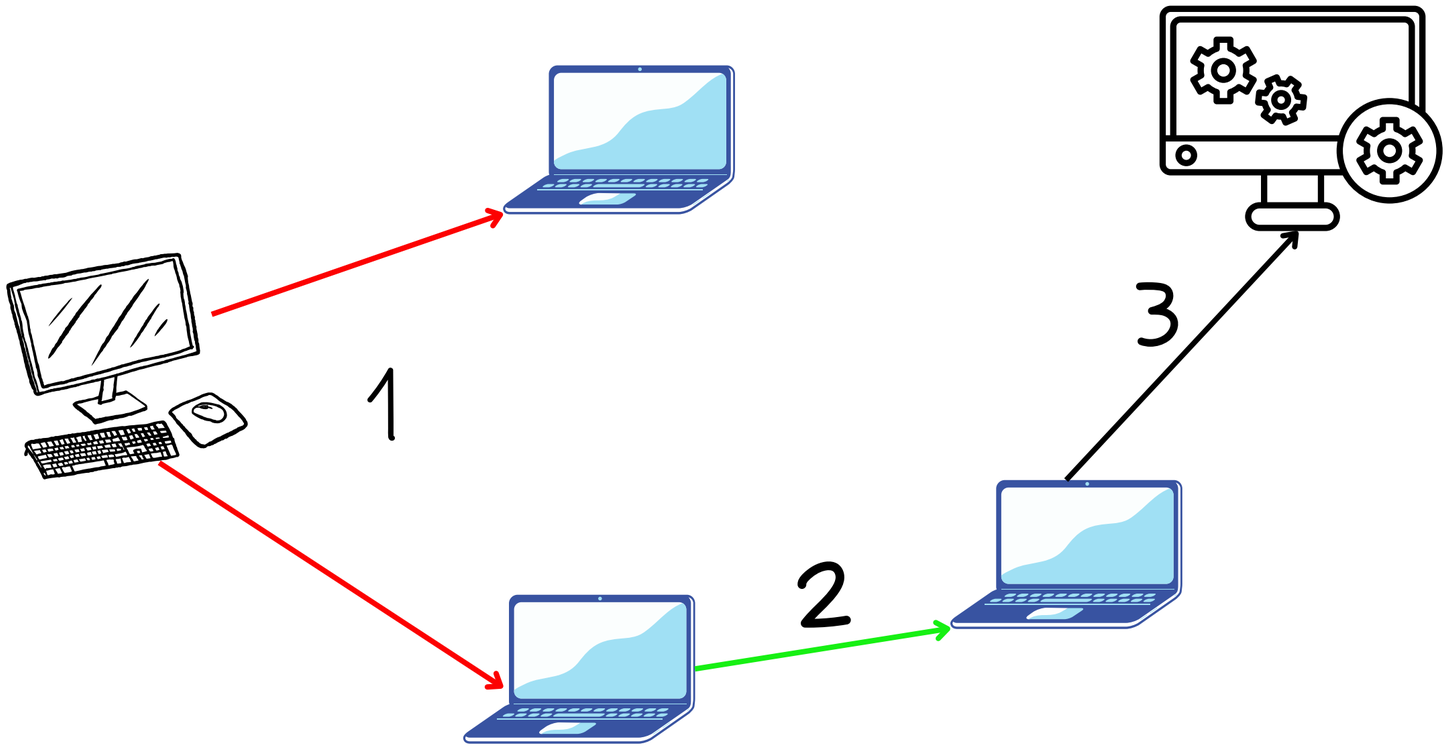


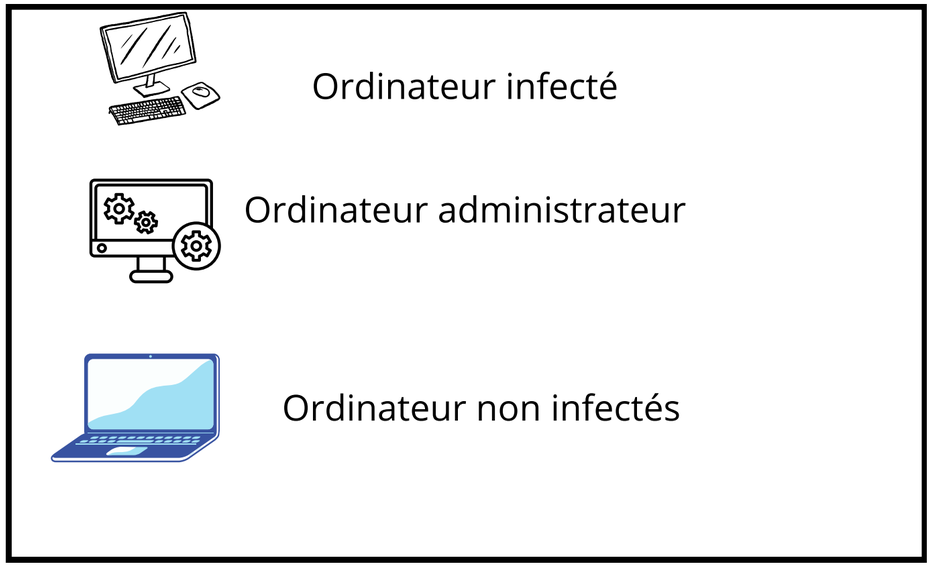
- Malware
- BackDoor
- Modifier paramètres sécurités

I. Procédés de l'attaque

I.III Élévations des privilèges et actions

Mouvement latéral





I. Procédés de l’attaque

I.III Élévations des privilèges et actions

Annonce de l’attaque

1 2 3

1 Avant annonce

2 Cryptage données

3 Demande rançon

Source : jvs-mairistem.fr et bocassay.com

II. Comment s’en protéger

II.I Devenir invisible

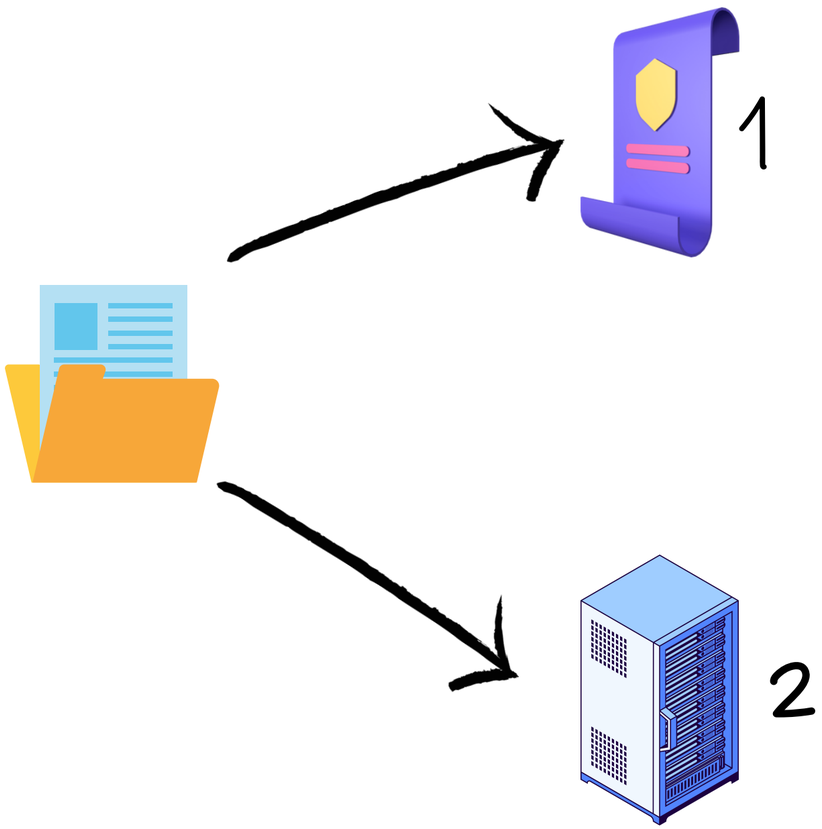
II.II Analyses régulières

II.III Isolation et Sauvegardes

II. Comment s’en protéger

II.I Devenir invisible

La confidentialité



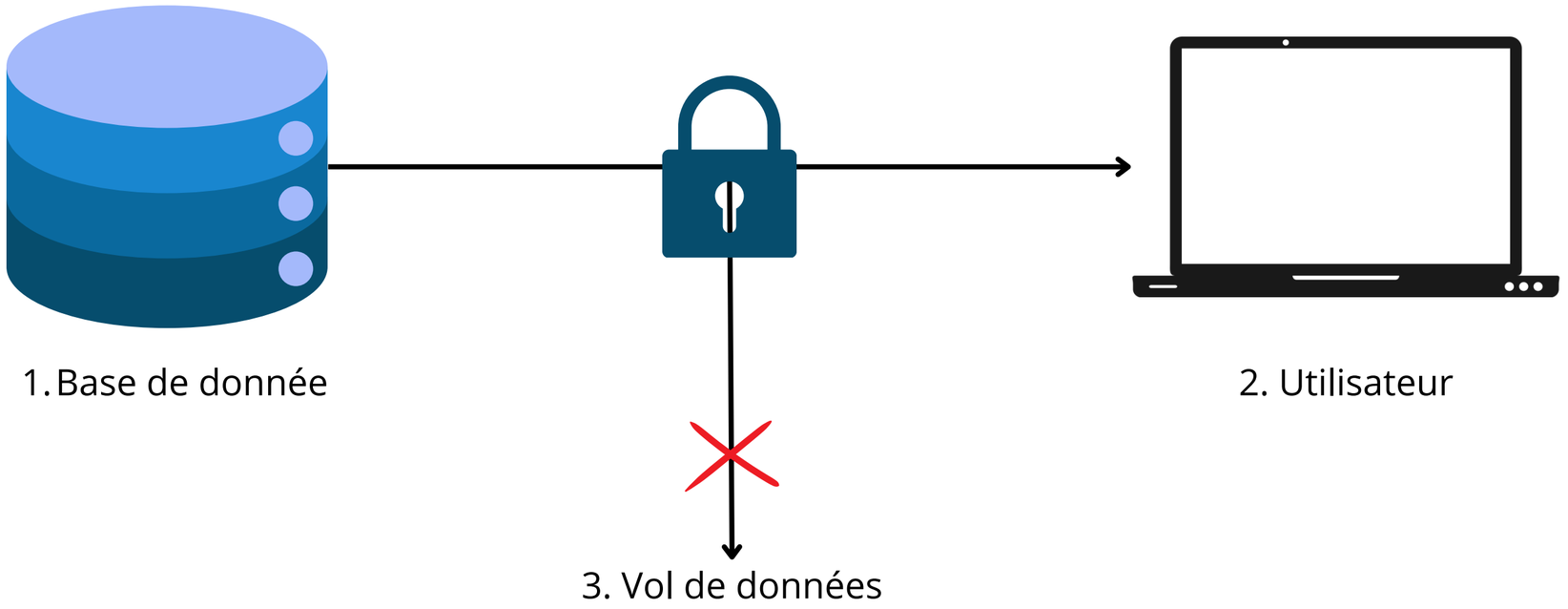
1 Règlement stricte

2 Données cryptées

II. Comment s’en protéger

II.I Devenir invisible

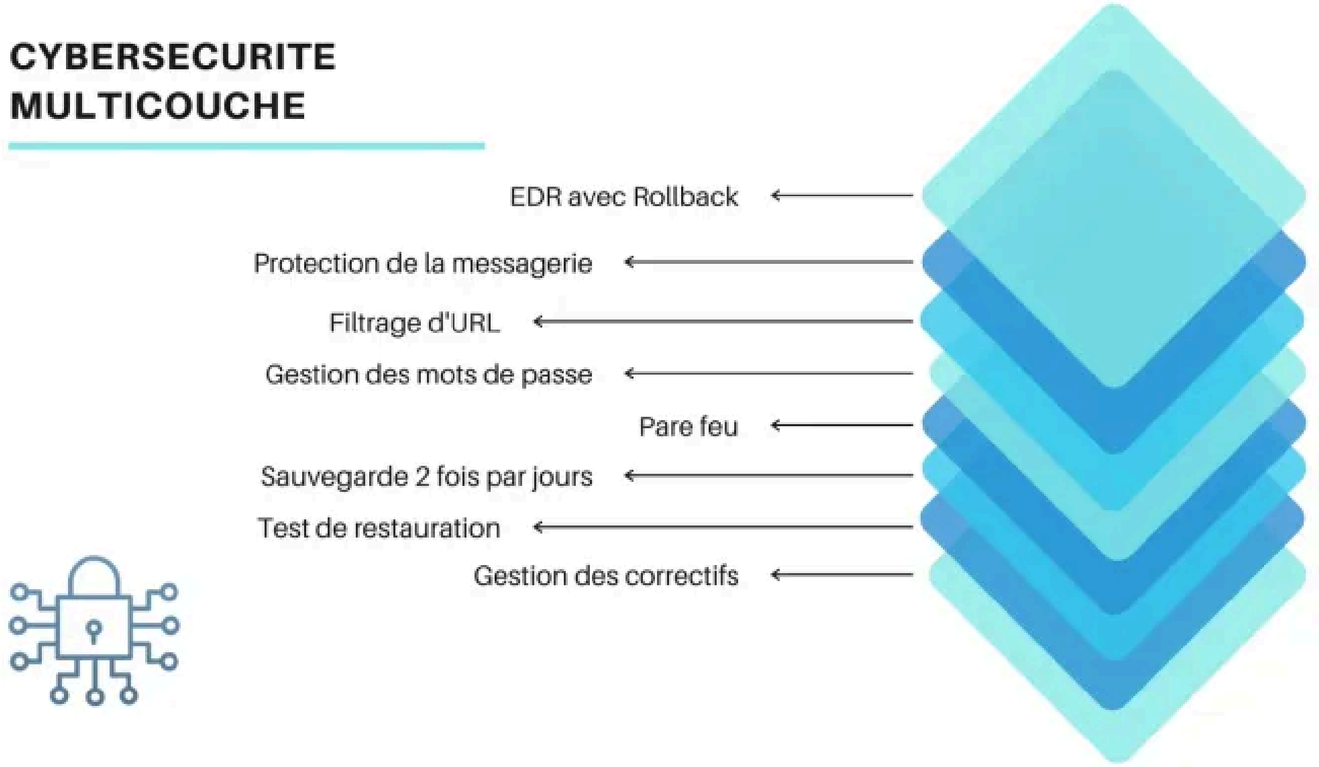
L’intégrité



II. Comment s’en protéger

II.II Analyses régulières

- Adopter une approche multicouche



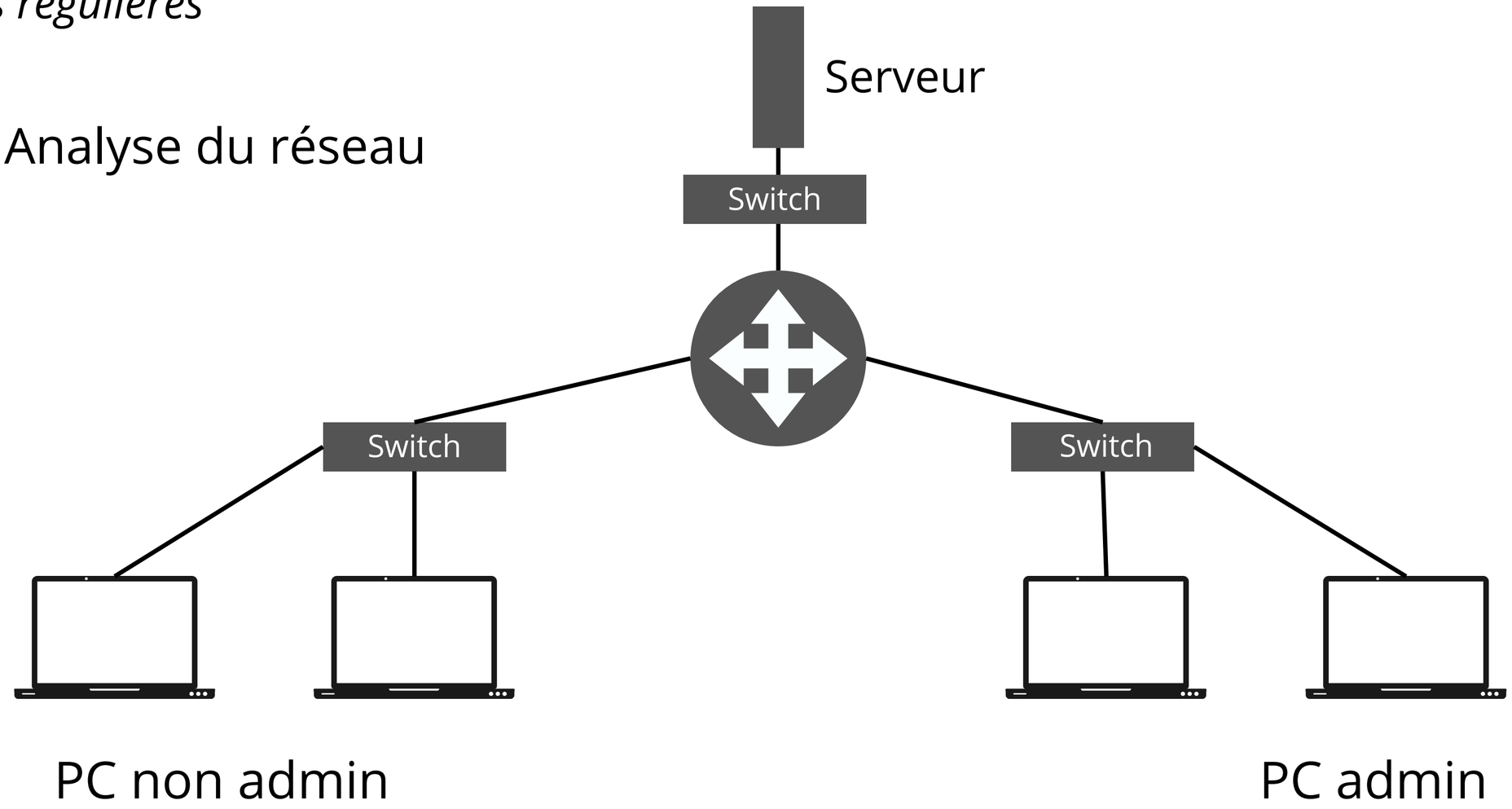
Source : oecy.io/cybersecurite

II. Comment s’en protéger

II.II Analyses régulières

- Analyse du réseau

Schema d’un réseau

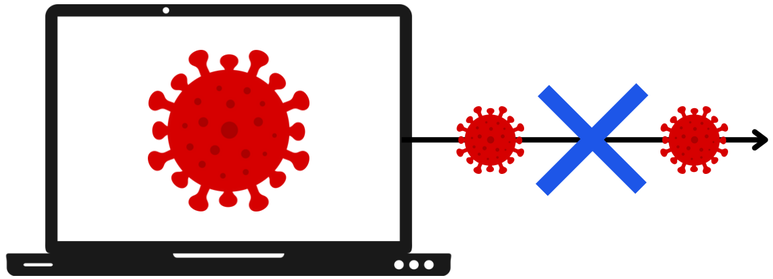


II. Comment s’en protéger

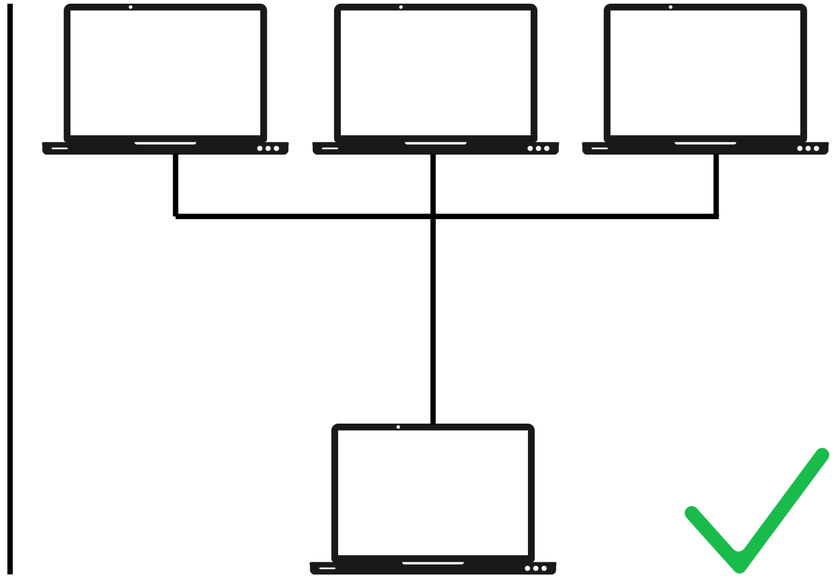
II.III Isolation et Sauvegarde

Isolation

1. Appareil isolé



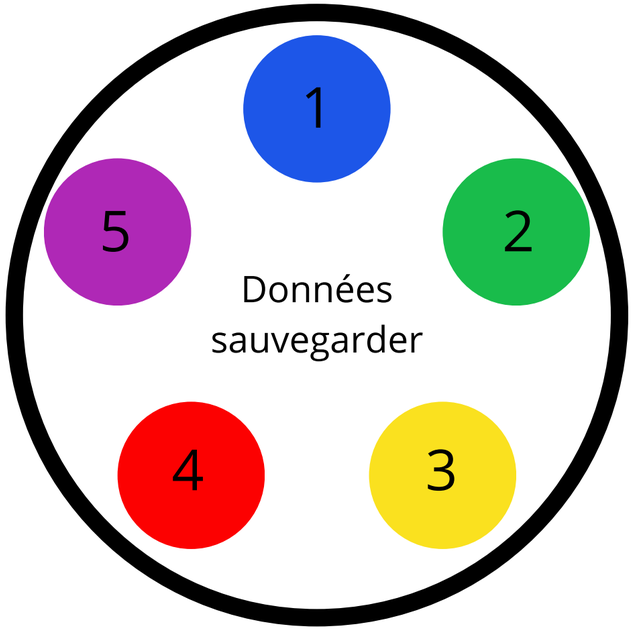
2. Reste du réseau



II. Comment s’en protéger

II.III Isolation et Sauvegarde

Sauvegarde



1. Type de données à sauvegarder
2. Objetctif du temps de récupération
3. Objectif du point de récupération
4. Exigence de stockage
5. Sécurité

Conclusion:

- **Procédés de l’attaque**
  - Repérer la cible
  - Infecter la cible et s’implanter durablement
  - Mise en action

- **Comment s’en protéger**
  - Rester imperméable
  - S’assurer de la sécurité du réseau
  - Limiter les pertes en cas d’attaque