Almond

Ransomware

Digital & Technology
Information Security
Almond Institute

CLUSIS

Transform, Secure & Beyond

07/02/2023

Agenda

- 1- La place du ransomware parmi les menaces cyber
- 2- Les étapes d’une attaque par ransomware
- 3- Comment se protéger ?
- 4- Et vous ? Où est ce que vous en êtes ? → Le Diagnostique

La place du ransomware parmi les menaces Cyber

La place du ransomware parmi les menaces cyber

Panorama: attaques croissantes et impactantes

Des hackers de plus en plus efficaces

Des enjeux et intérêts croissants

Des entreprises vulnérables

POURQUOI UN TEL DÉVELOPPEMENT ?

La généralisation du télétravail et l'augmentation des crises cyber liée aux nouveaux risques (accélération de la transformation digitale).

Des attaques de plus en plus amples et virulentes

> **65 % selon le NCSC**
d'augmentation d'attaques en 2021, un chiffre supérieur à la moyenne mondiale

> **21'714 signalements**

- Escroquerie : 11'300
- fraude au paiement anticipé : 2'704
- la fraude à l'investissement 397
- l'arnaque au président : 394

> **+ 30%**
4'498 sites de phishing signalés sur le portail antiphishing.ch, géré par le NCSC

> **20%**
des fuites de données commencent par une compromission d'identifiants

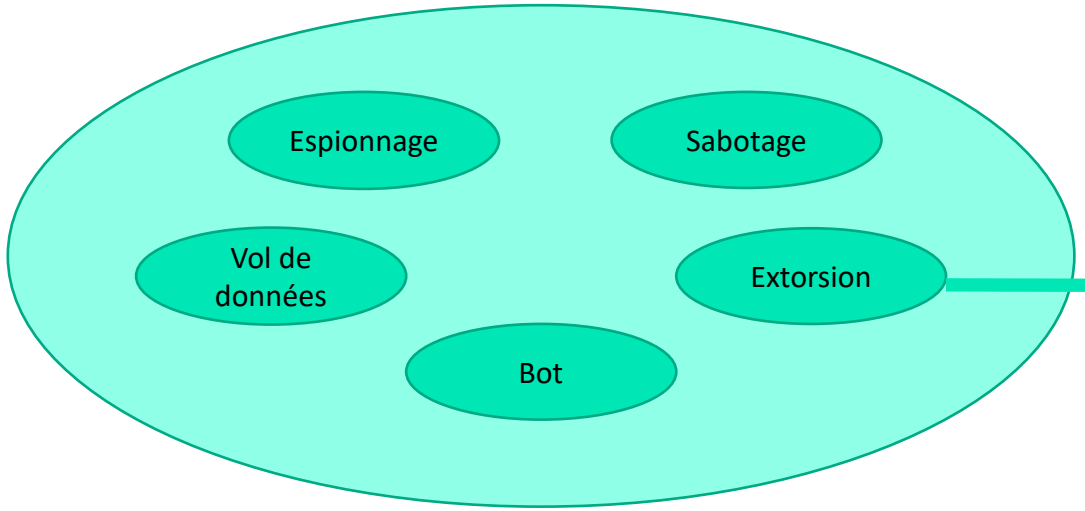
- **4,62 millions $**
coût moyen d'une attaque par ransomware

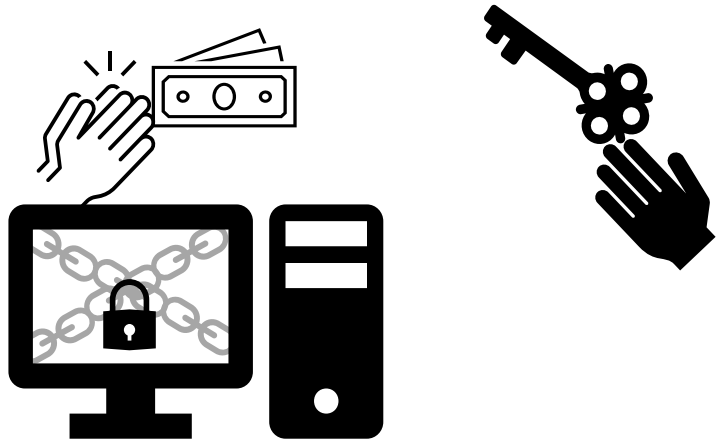
Les incidents recensés dans la presse ne représentent que 10% des incidents réels !

« 80 % de la cybercriminalité est liée à **des bandes organisées** transfrontalières et représente un coût financier **plus important que les coûts combinés des trafics de cocaïne, marijuana et héroïne** » (Interpol)

La place du ransomware parmi les menaces cyber

Pourquoi se focaliser sur le ransomware ?





> Pourquoi se focaliser sur le ransomware?

- L'attaque avec le plus d'impact ⚠
- 66% des crises sont dues à une attaque par ransomware
- Les ¾ combinent blocage du SI et vol de données

> Ransomware

- Logiciel malveillant de demande de rançon
  - > Chiffrement des données
  - > Blocage du Système d'Information
  - > Chantage de divulgation

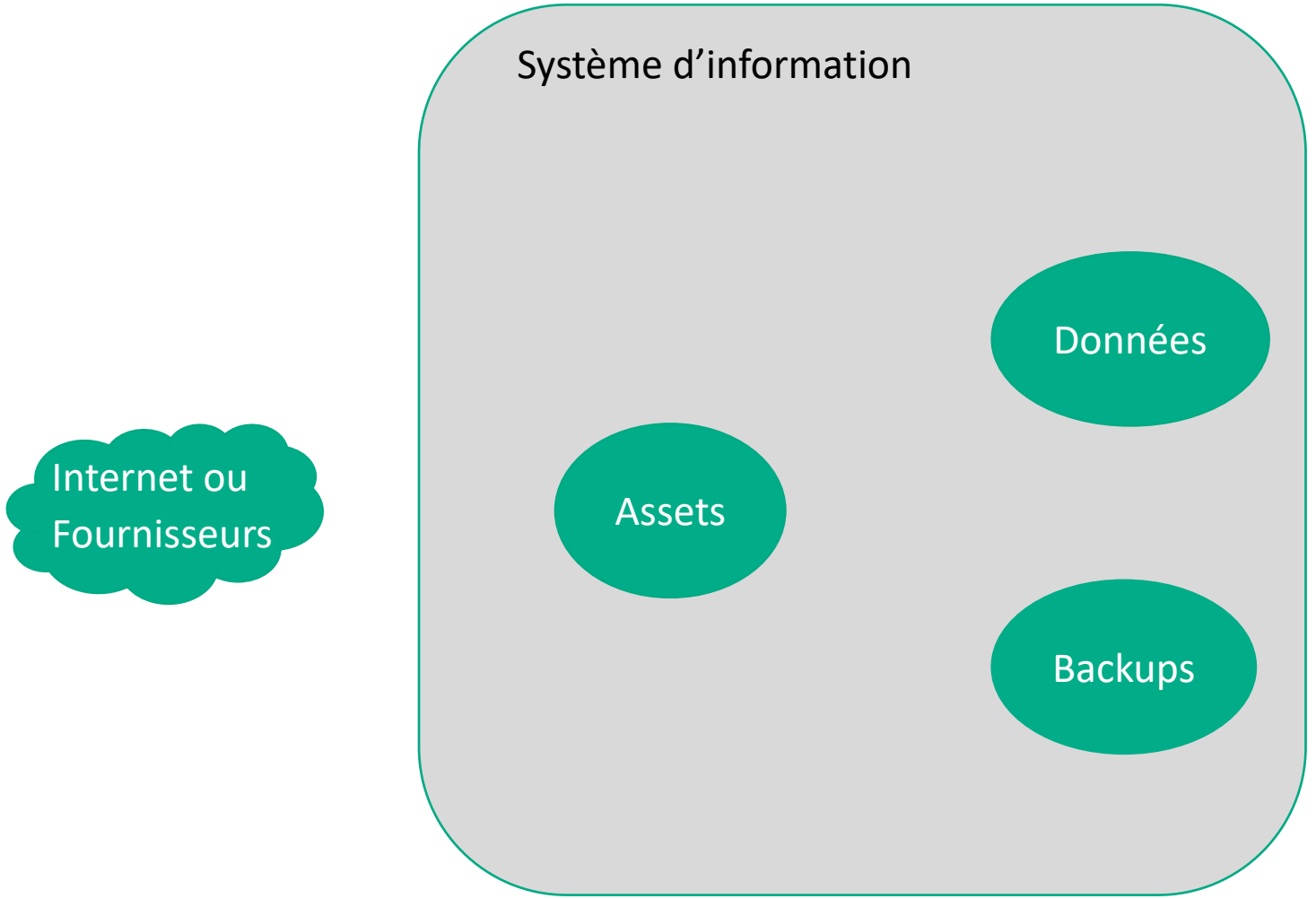
Data sources: CESIN & ENISA

Les étapes d’une attaque par ransomware

Les étapes d’une attaque par ransomware

L’environnement

> Environnement générique
  - Internet ou fournisseurs
  - Des assets
  - Des données
  - Des backups sur site ou hors site



Les étapes d’une attaque par ransomware

Reconnaissance

> Récupération d’information autour de la cible

- Chartre graphique
- Adresses emails
- Évènements
- Organigramme

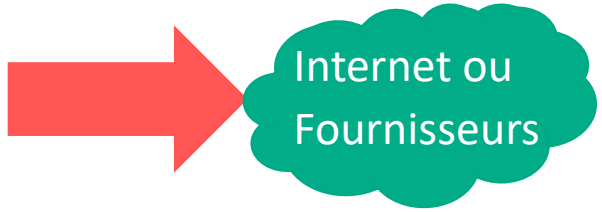
Phishing ciblé

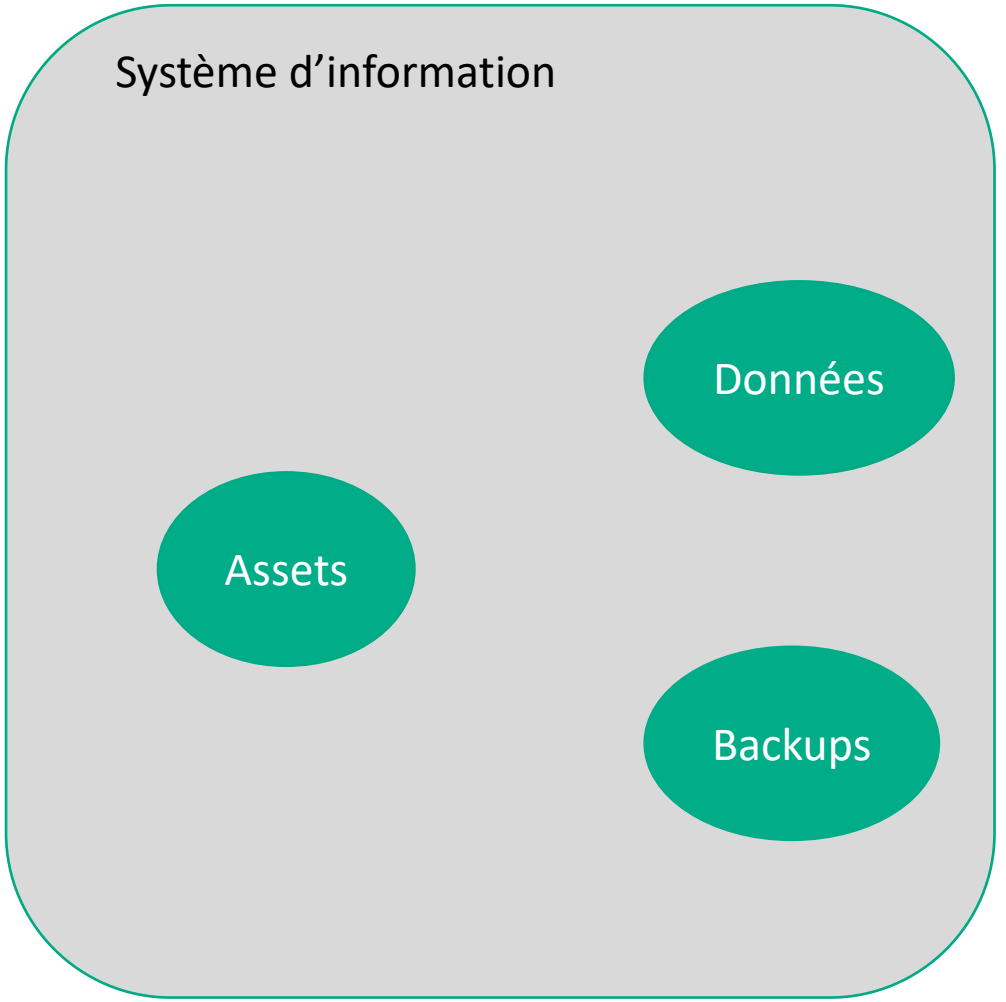
- Cartographie réseau
- Adresses IP, nom de serveurs
- Technologies utilisées et versions
- Mots de passe
- Toute information utile

- Exploitation de vulnérabilité ou de mauvaises configurations

- Simplification des étapes suivantes

Reconnaissance

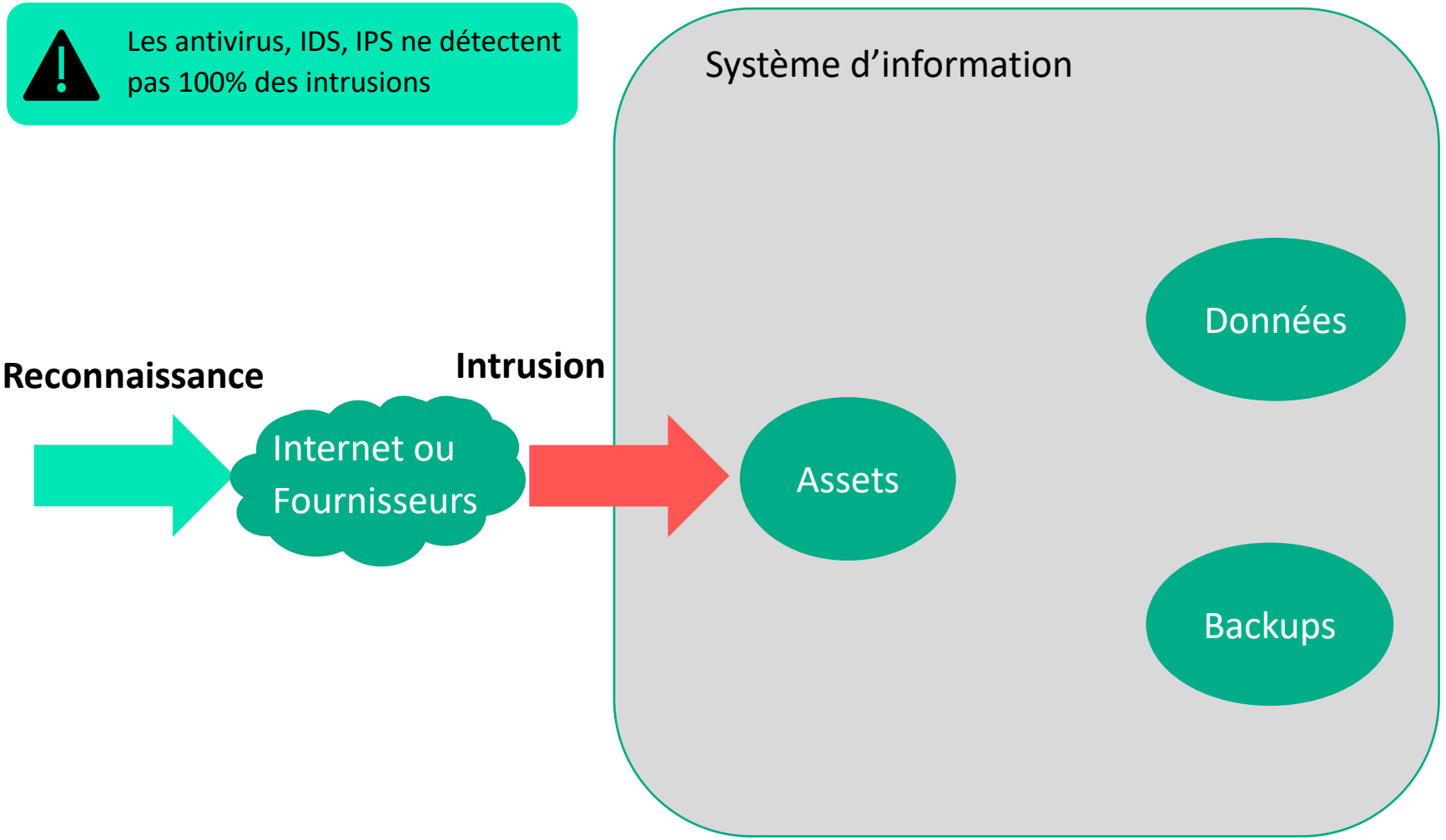




Les étapes d’une attaque par ransomware

Intrusion :Principaux canaux

- Phishing
  - 33% des intrusion sont faites par phishing (coveware)
  - Premier vecteur d’attaque dans les entreprises (CESIN & ENISA)
- Exploitation de vulnérabilité
  - Patch critique non appliqué à temps
- Exploitation d’un port réseau exposé (RDP)
  - 50% des intrusions sont réalisés par une compromission d’un port RDP pour les entreprises de moins de 10 000 personnes (Coveware)
- Autre point d’entrées
  - USB
  - WiFi
  - VPN
  - etc



Les étapes d'une attaque par ransomware

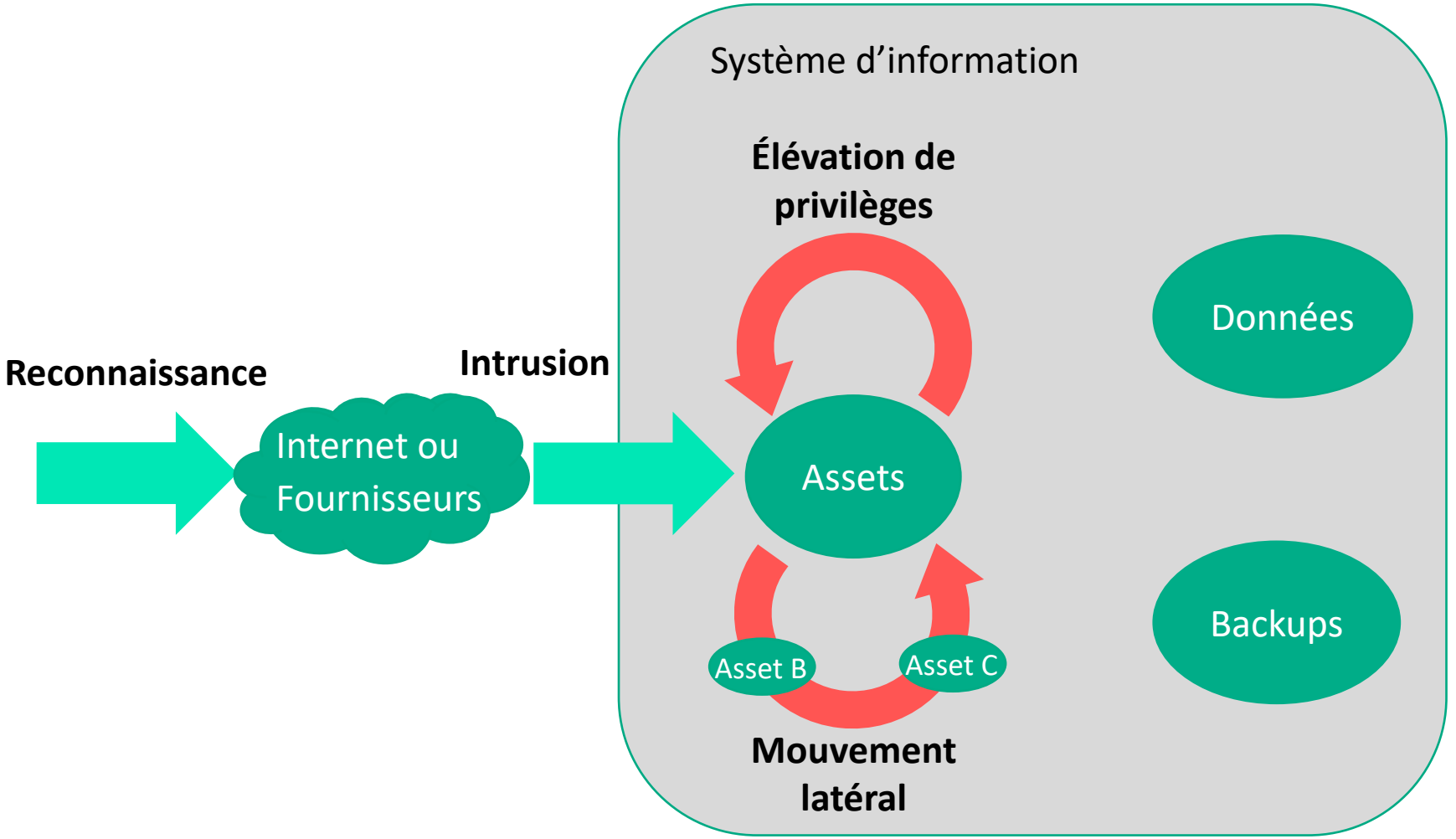
Élévation de privilège & mouvement latéral

> Élévation de privilège

- Exploitation de **l'annuaire** (Active Directory)
- Vulnérabilité ou mauvaise configuration des asset
- Utilisation de protocoles faibles ou non chiffrés
- Mot de passe faible

> Mouvement latérale

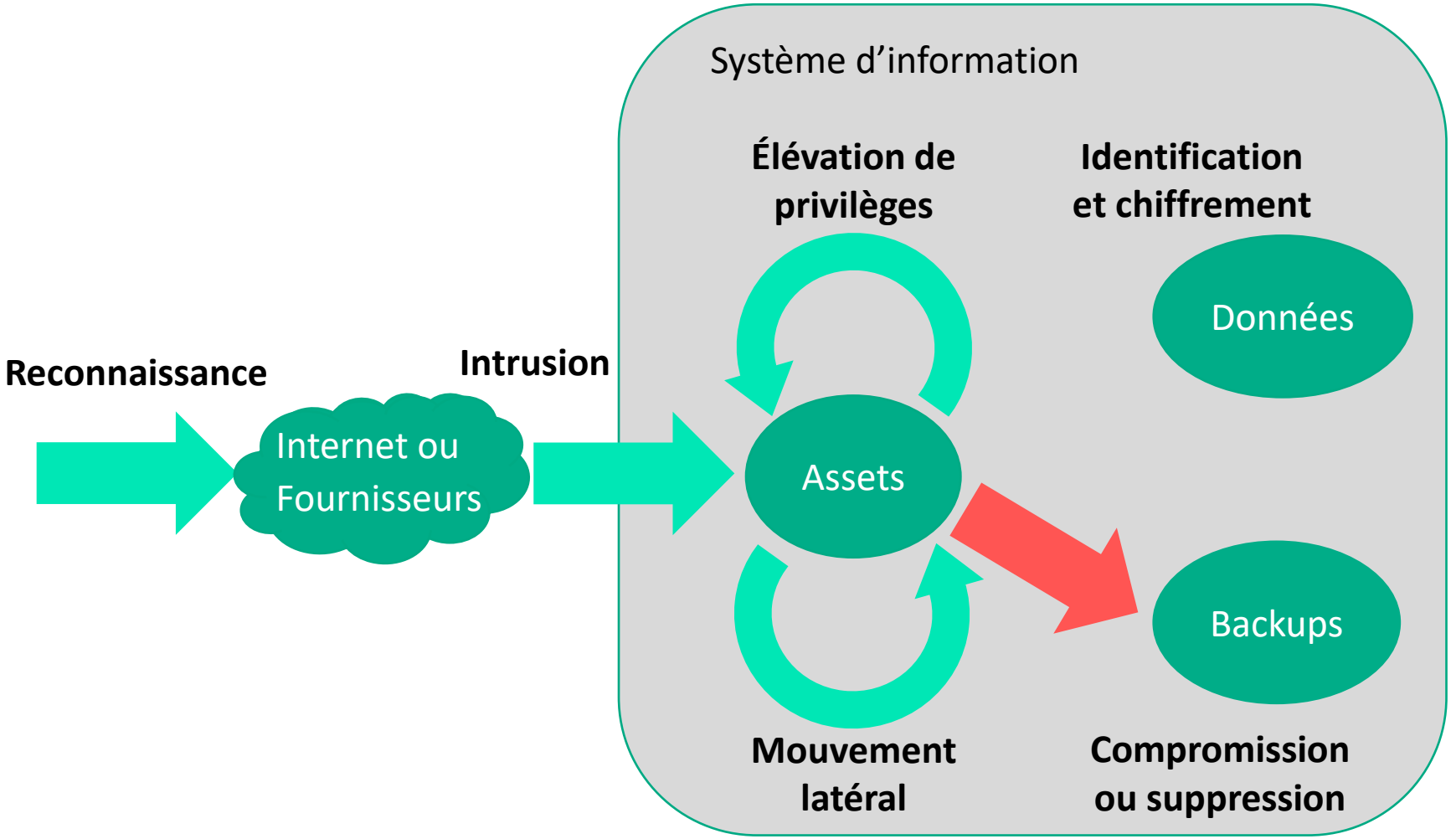
- Reconnaissance intérieur
- Mauvais cloisonnement du système d'information
- Principe du moindre privilège non appliqué



Les étapes d'une attaque par ransomware

Compromission des backups

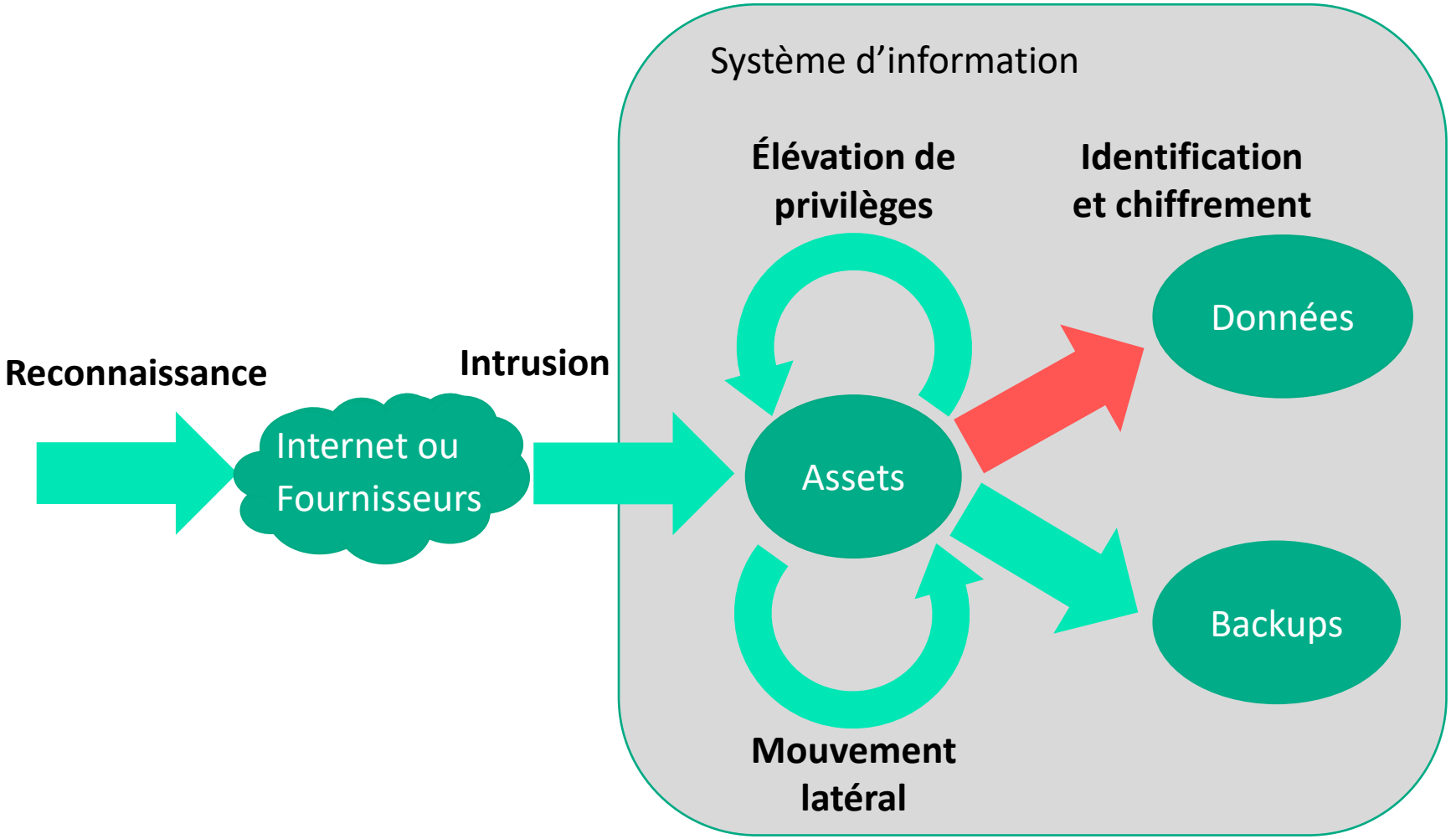
- Suppression de tout les backups accessibles (shadow copy, etc)
- Désactivation des services de backup



Les étapes d'une attaque par ransomware

Identification et chiffrement des données

- Identification des données critiques
- Chiffrement
- Exfiltration des données
  - Revente
  - Pression de divulgation



Comment se protéger ?

Comment se protéger ?

2 principes

1 Mettre des mesures de sécurité sur l'ensemble de la chaine

Couvrir l'ensemble de la chaine d'attaque

> Avoir au moins une protection pour chaque étape :

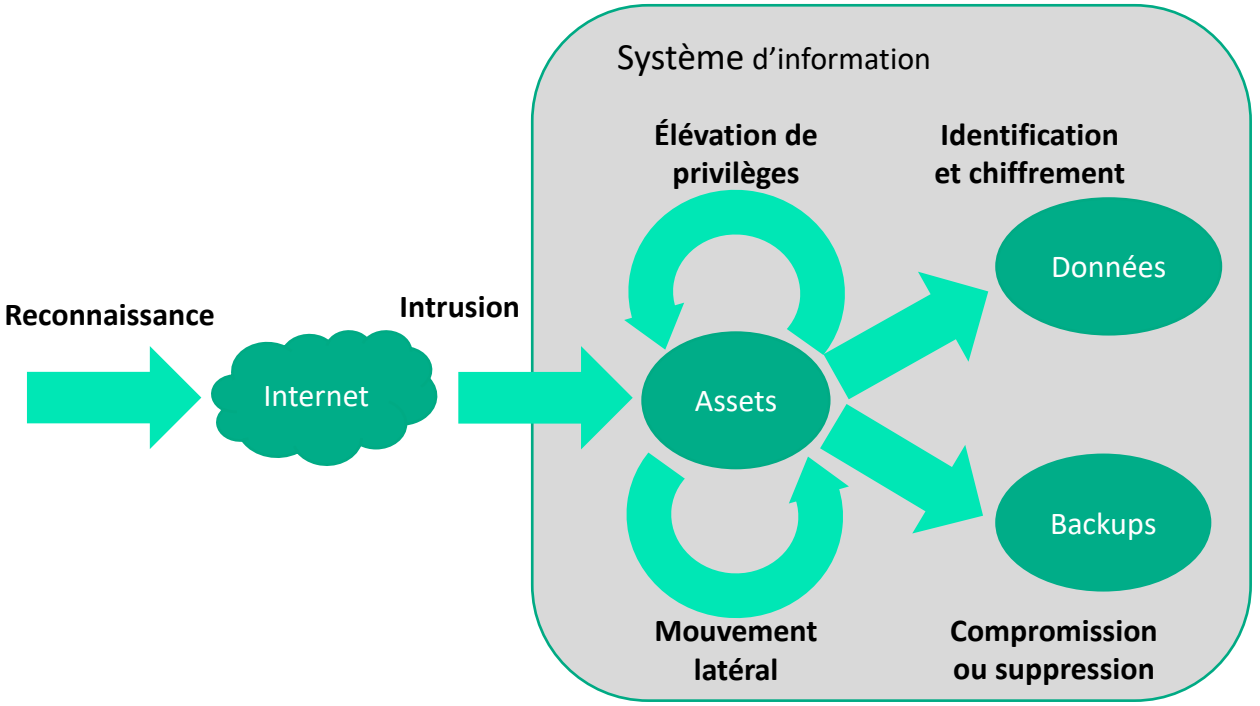
- Reconnaissance
- Intrusion
- Élévation de privilèges
- Mouvement latéral
- Compromission des backups
- Identification et chiffrement des données

2 Adopter une approche de défense en profondeur

Ne pas se reposer sur une seule mesure

> Déployer différentes mesures pour chaque étape afin :

- D'identifier
- Protéger
- Détecter
- Répondre
- Restaurer

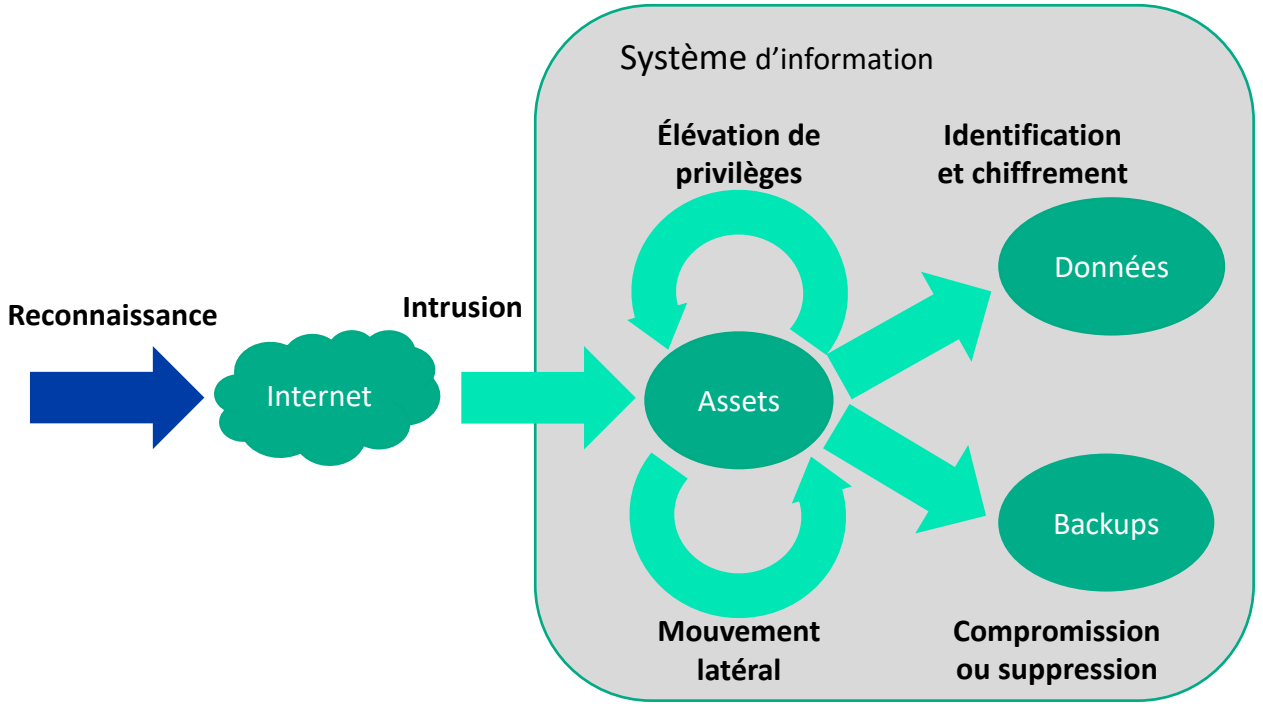


Comment se protéger ?

Reconnaissance

> Connaitre et maitriser les risques liés aux données publiques

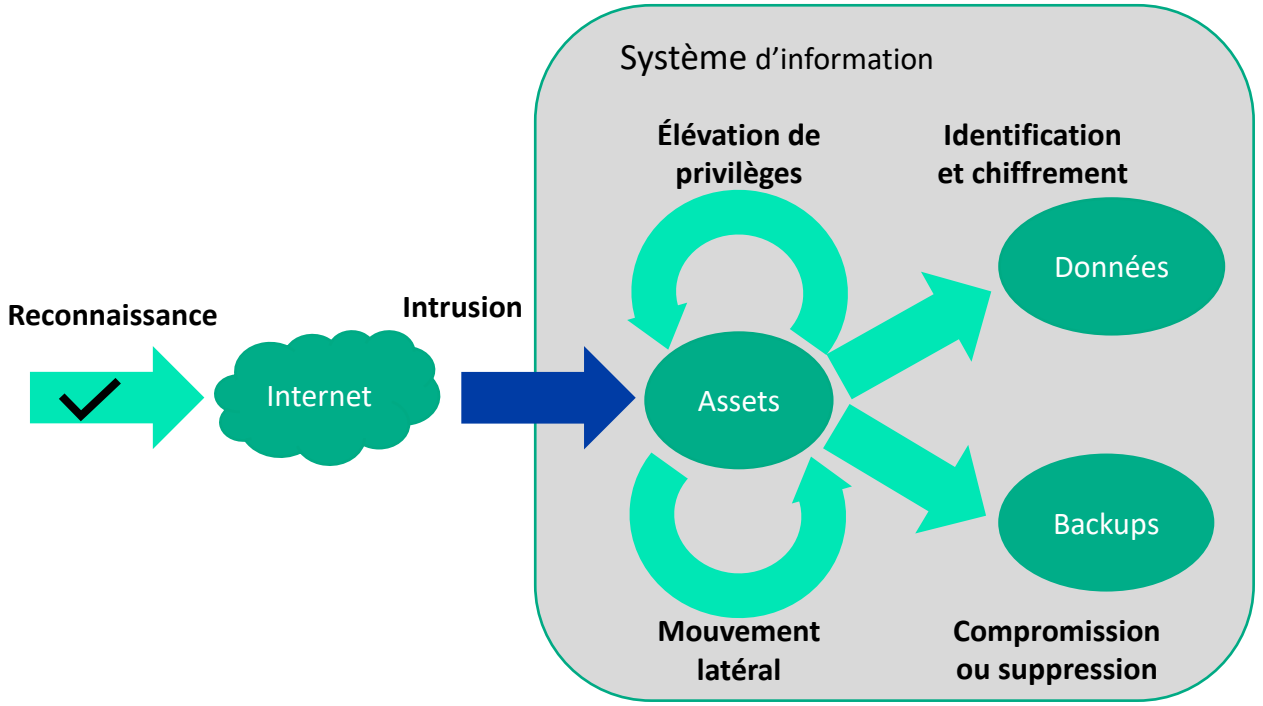
- Classifier ses données
- Protéger les données sensibles
- Faire une revue régulière des informations présentes publiquement



Comment se protéger ?

Intrusion

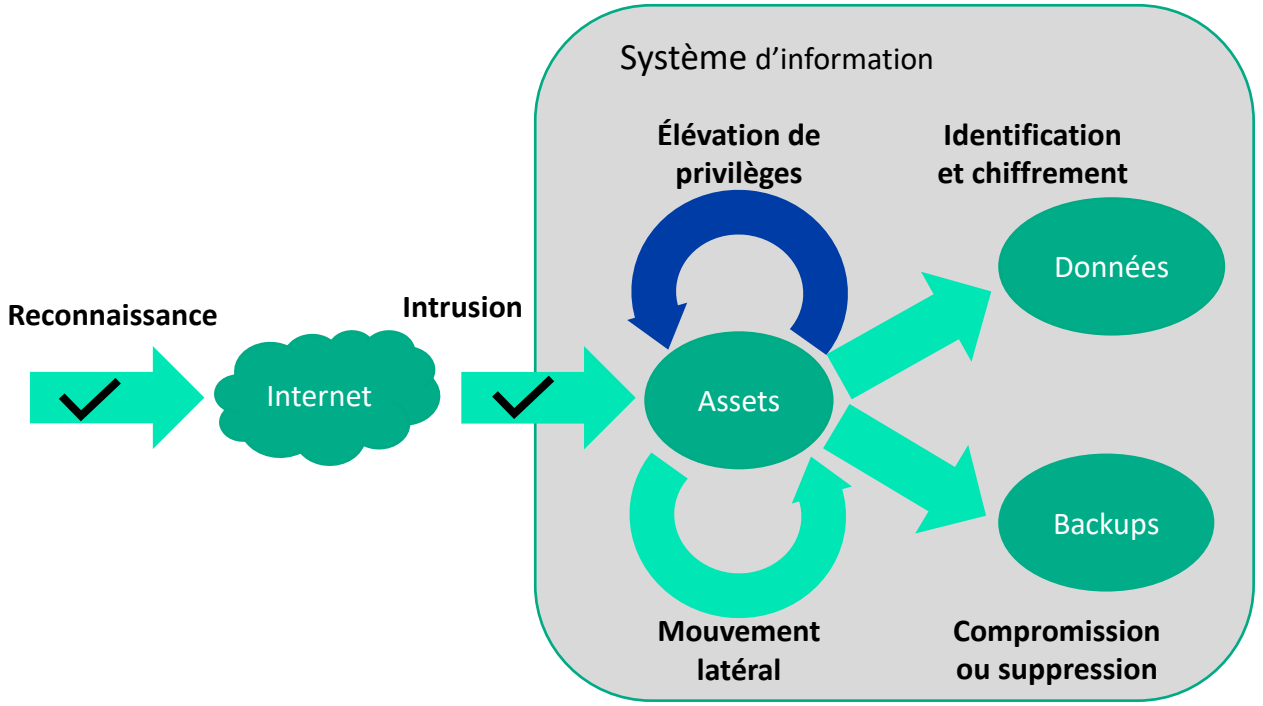
- Limiter les intrusions sur les services exposés
  - Cartographier les assets sensibles
  - Maintenir à jour les systèmes et logiciels
  - Utiliser et maintenir à jour les logiciels antivirus
  - Revoir les configurations réseaux (firewall, ports sensibles exposés)
- Limiter les intrusions chez les collaborateurs
  - Sensibiliser les collaborateurs
  - Renforcer la sécurité des postes de travail (antivirus, EDR, etc)
  - Renforcer les filtres et contrôles sur le mail et la navigation web
  - Avoir une authentification forte
- Détecter les intrusions
  - Avoir et utiliser un outil de détection d'intrusion
  - Contrôler les accès au réseau
  - Centraliser et corréler les logs



Comment se protéger ?

Élévation de privilèges

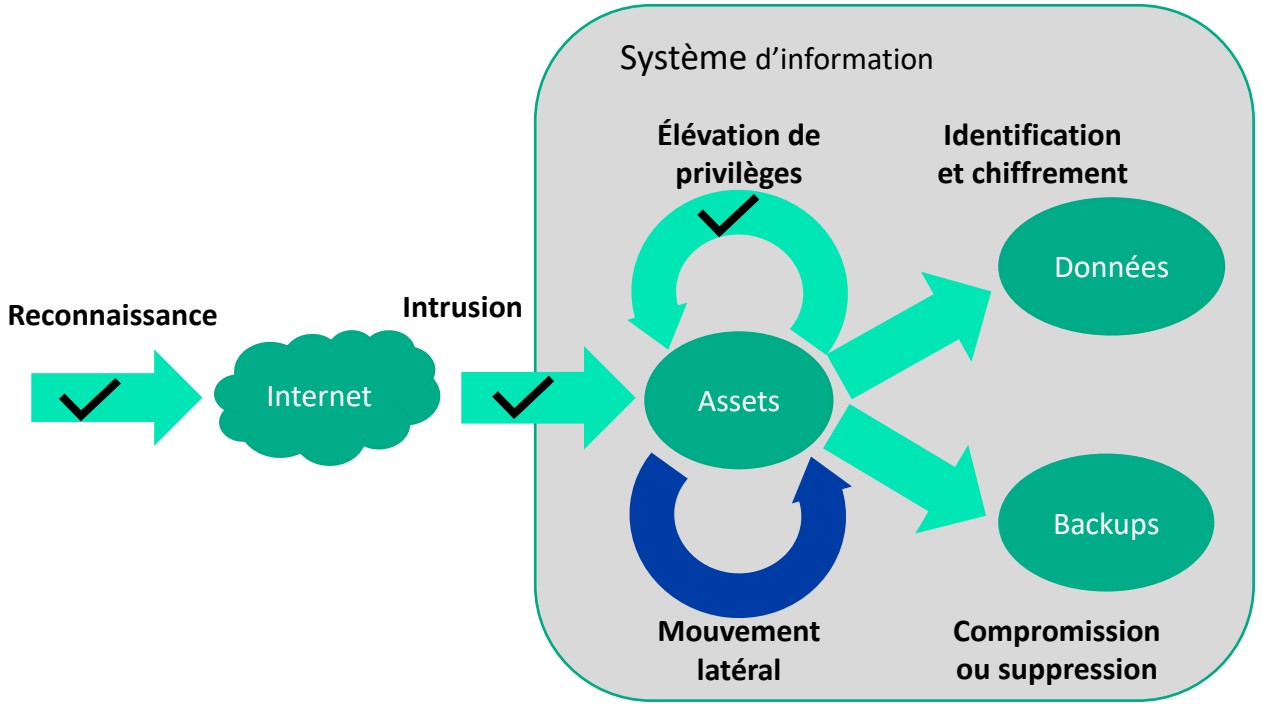
- Protéger les comptes à privilèges
  - Sécuriser son annuaire ⚠
  - Maintenir à jour les systèmes et logiciels
    - Savoir corriger rapidement les vulnérabilités les plus critiques
  - Avoir une bonne gestion des mots de passes
    - Complexité
    - Rotation
    - Stockage
    - Accès
- Détecter une mauvaise utilisation d'un compte à privilèges
  - Traçabilité
  - Non répudiation
  - Détection des actions malveillantes



Comment se protéger ?

Mouvement latéral

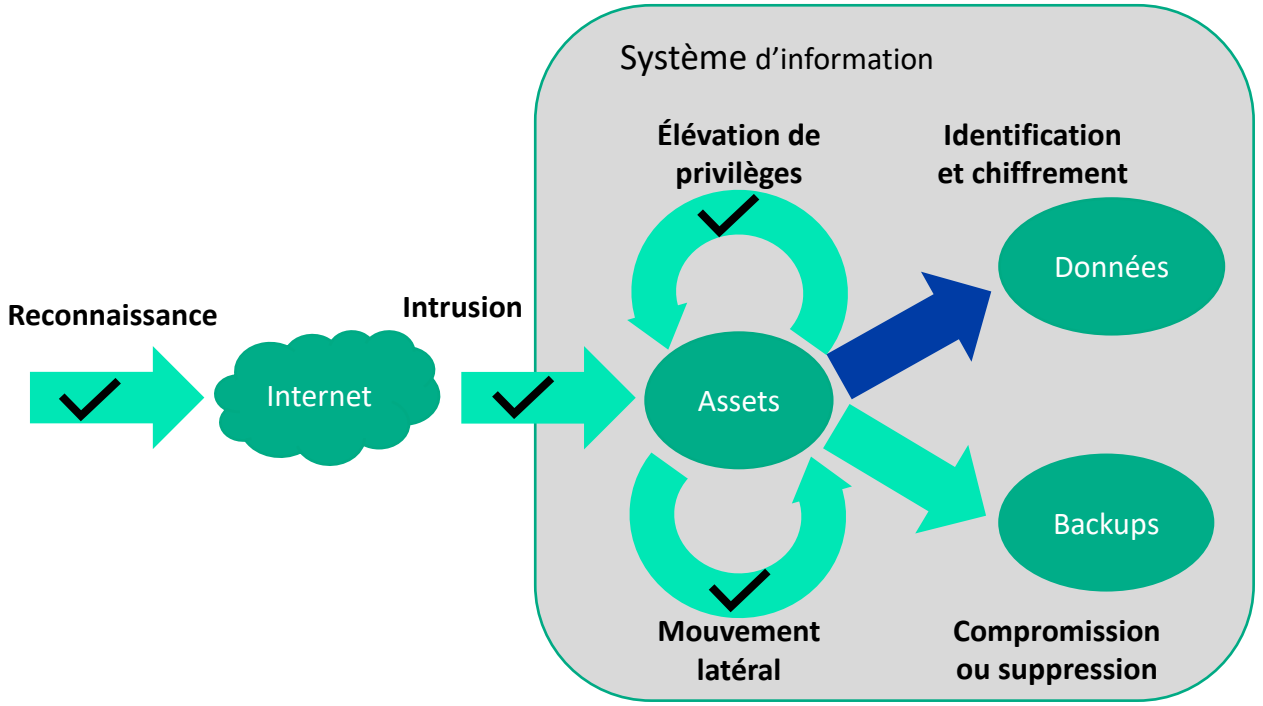
- Limiter l'accès aux composant critiques
  - Cloisonner le système d'information
  - Isoler les composants les plus critiques
  - Limiter les droits et autorisations des utilisateurs et administrateurs aux systèmes et applications en fonction de leur tâches
    - Avoir plusieurs comptes d'administration pour chaque taches ⚠



Comment se protéger ?

Identification et chiffrement des données

- Savoir où sont ses données sensibles
  - Cartographier les assets sensibles
- Renforcer la sécurité des données sensibles
  - Donner les accès aux personnes strictement nécessaires
  - Donner les droits nécessaire à la réalisation des taches (lecture, écriture, exécution)
  - Chiffrer les données
- Limiter la sortie d'information
  - Maitriser les accès internet

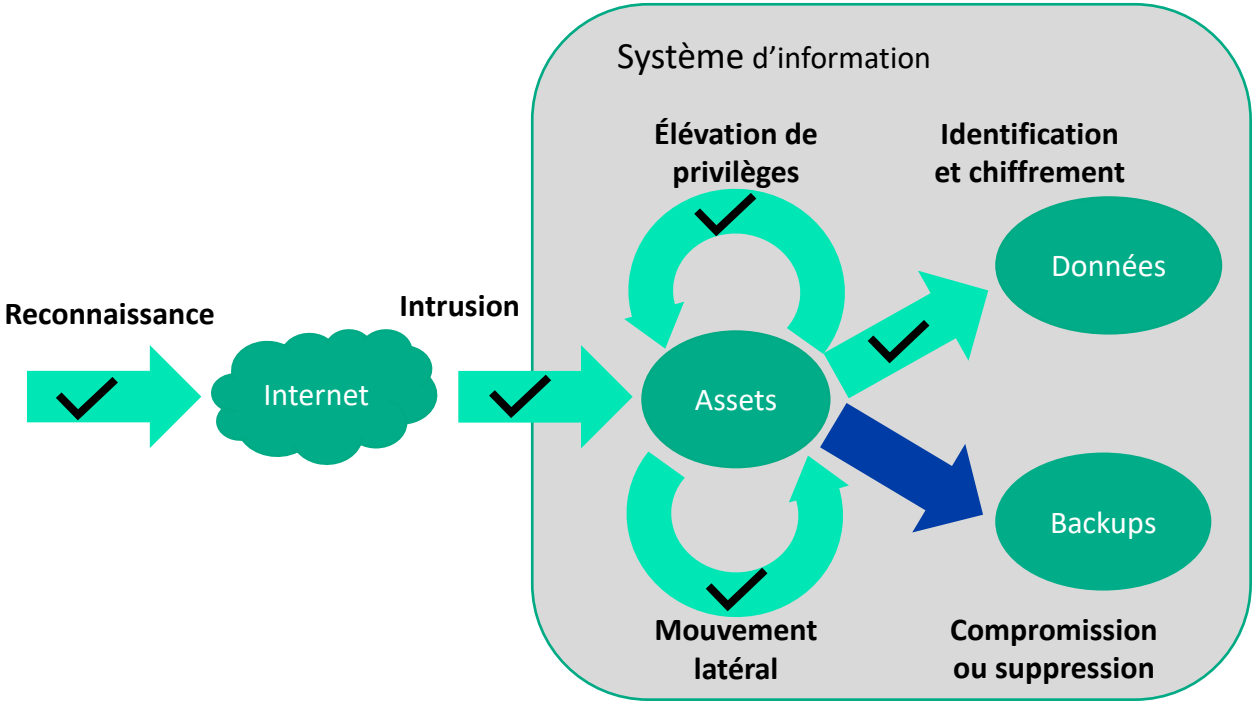


Comment se protéger ?

Compromission des backups

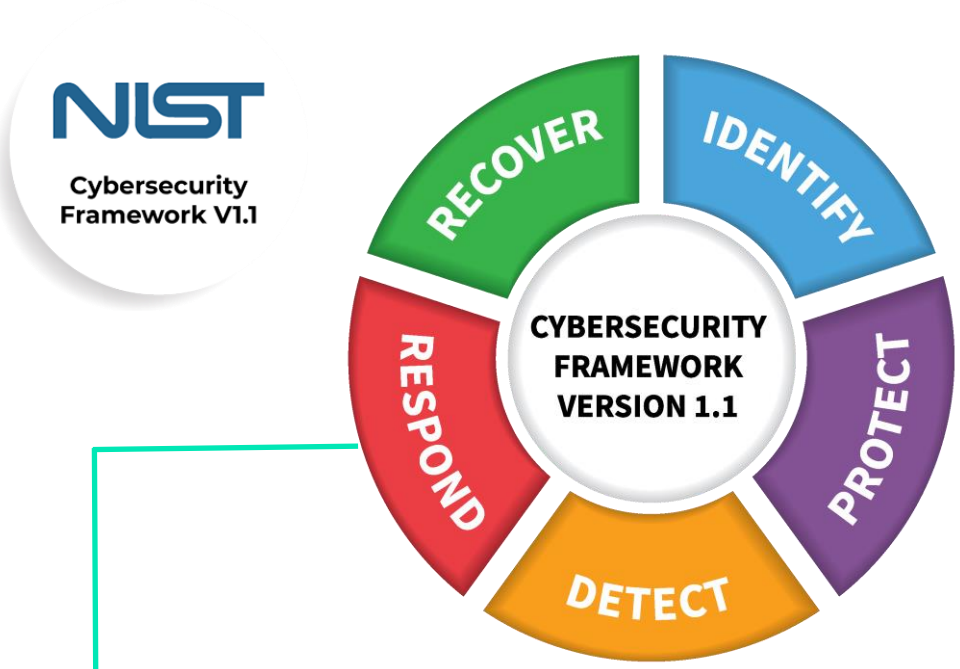
> Pouvoir restaurer son Système d'Information en cas d'attaque

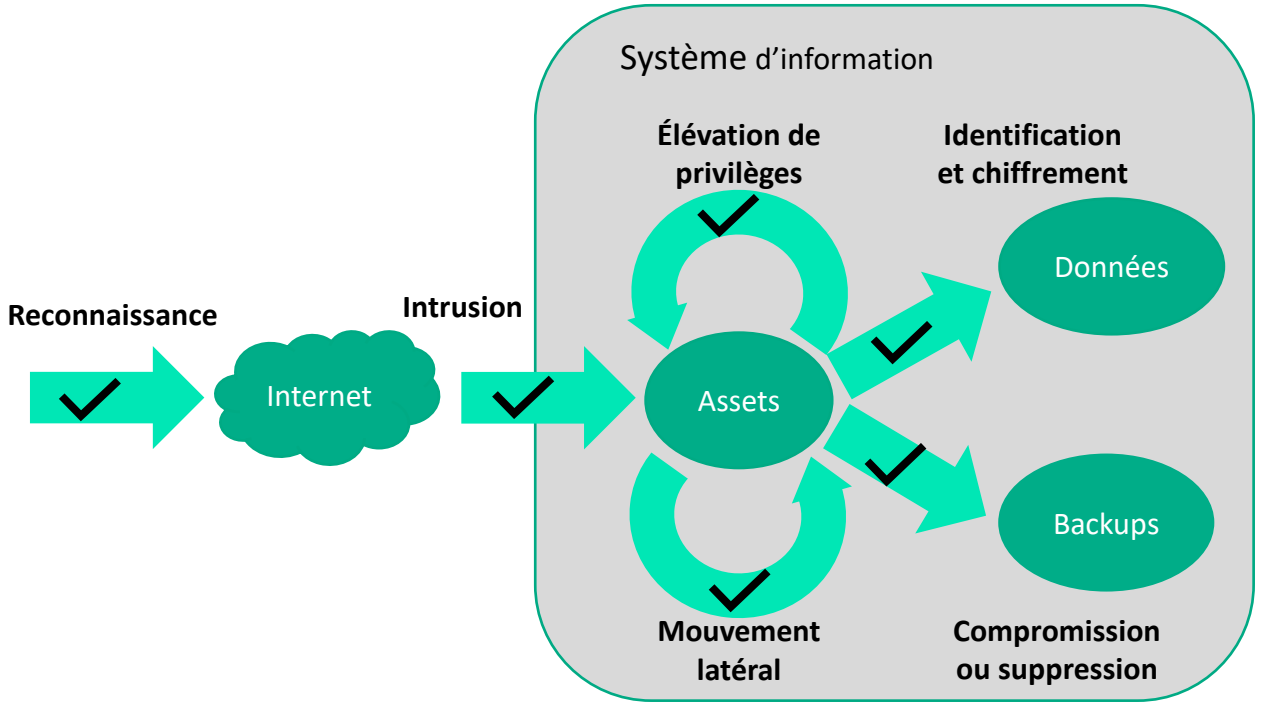
- Avoir identifié les données importantes à sauvegarder
- Réaliser des sauvegardes récurrentes
- Avoir une longue durée de conservation
- Sauvegarder dans une zone isolée
- Avoir des sauvegardes non effaçables
- Réaliser de tests récurrents de restauration des données



Comment se protéger ?

Se préparer grâce à un Framework comme le NIST





Respond :

- Mettre en place un plan de réponse aux cyberattaques
- Penser à sa stratégie de communication de crise cyber
- Évaluer l'opportunité de souscrire à une assurance Cyber
- Auditer son système d'information
- N'hésitez pas à vous faire accompagner par des experts dans le domaine

Où est-ce que vous en êtes ?

Où est-ce que vous en êtes ?

Notre vision du diagnostique de sécurité avec les partenaires du Clusis

- Diagnostique axé autour des étapes ransomware
  1. Compréhension de vos **enjeux métiers**
  2. Réalisation d'un **diagnostique** de sécurité autour de vos enjeux métiers

- Proposition de mesures pour couvrir les risques identifiés
  3. Proposition d'une **feuille de route** afin de renforcer la sécurité au regard de vos **enjeux métiers** et des **étapes ransomware**

merci

Gabriel LEPERLIER
Partner – Directeur Associé
gleperlier@almond.eu

https://almond.consulting

Paris
Bâtiment Crisco Duo
7 avenue de la Cristallerie
92310 Sèvres
E. contact@almond.consulting
T. +33 (0)1 46 48 26 00

Nantes
Centre d'affaires Euptouyou
Immeuble Asturia C
4 rue Edith Piaf - 44800 Saint-Herblain
E. contact@almond.consulting
T. +33 (0)2 55 59 01 10

Strasbourg
Centre d'affaires Regus les Halles
Tour Sébastopol
3 quai Kléber - 67000 Strasbourg
E. contact@almond.consulting
T. +33 (0)1 46 48 26 00

Lyon
Centre Regus Lyon Brotteaux
132 rue Bossuet
69006 Lyon
E. contact@almond.consulting
T. +33 (0)1 46 48 26 00

Genève
Route de la Galaise 11B
1228 Plan les Ouates
E. contact@almond.consulting
+41 (0) 22 588 96 98