DÉFENSE

(DANS LES TRÈS GRANDES LIGNES)

CONSTRUIRE UNE STRATÉGIE DE DÉFENSE

- « Solution magique » n’existe pas en cybersécurité
- N’importe quelle couche de protection peut tomber
- Et on doit supposer qu’elle **va effectivement** tomber
- De multiples niveaux de protection doivent être mis en place

PRÉVENTION VS. DÉTECTION

- **Prévention** ? Formidable. **Détection** ? Obligatoire.
- **Détection** ⇒ **réaction** ; on peut « minimiser les dégâts »
- Quand une attaque aura lieu avec succès, alors votre système de prévention sera *déjà en défaut*
  - Mais **pas de détection** ⇒ **pas de réaction** ; les conséquences peuvent alors être très graves
- Évidemment, si aucune réponse (réaction) n'est prévue, le système de détection n'a qu'une valeur tout relative

UN POINT SUR LES SCORES

- On estime que **90 % des attaques ne sont pas détectées**
- Parmi les 10 % restants, elles sont restées **indétectées pendant en moyenne 20 mois**
- En général, en SSI, le rapport d’investissements prévention/détection est beaucoup trop élevé

FLUX ENTRANTS VS. FLUX SORTANTS

- Plus de 95 % de surveillance se fait sur les flux entrants
  - Exfiltration de données ?
  - Centres de *Command & Control* (C2) ?
- De nouveau, on se concentre trop sur la prévention (principalement flux entrants) et pas assez sur la détection (beaucoup de flux sortants)

NOTION DE RISQUE

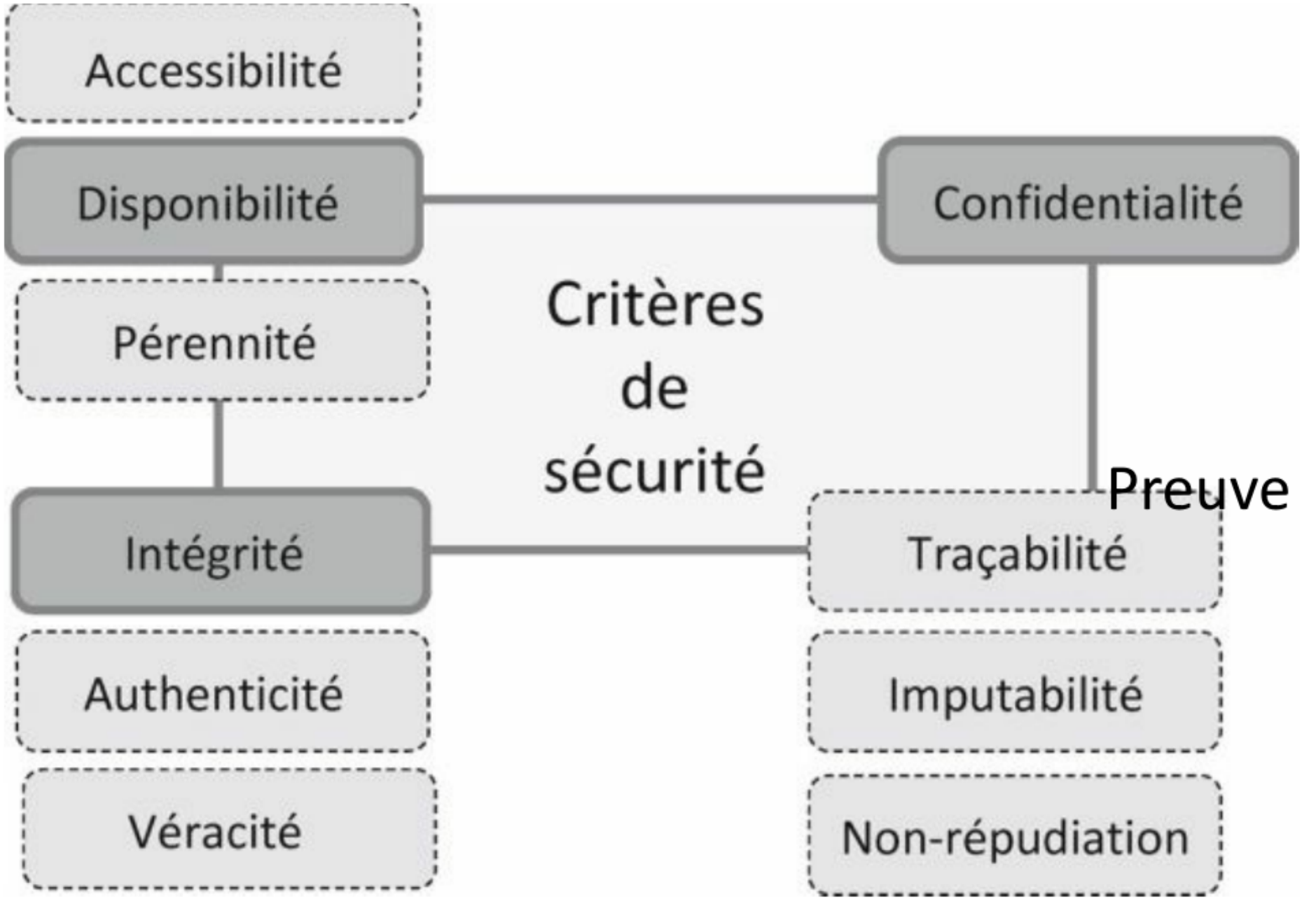
- Sécurité = gestion de risques sur les ressources critiques
- Cela induit les notions de :
  - **menaces** : potentiel de dommage pouvant arriver
  - **vulnérabilités** : failles qui permettent à ces menaces de se concrétiser
- **Risque = Menace x Vulnérabilité** (pour l'instant)
  - **on ne peut contrôler que les vulnérabilités**
  - vulnérabilité est **sans importance si aucune menace associée**

GESTION DES RISQUES 101

Avant de passer une minute ou de dépenser un euro sur une solution quelconque de cybersécu, toujours se poser ces 3 questions :

1. Quel est le risque auquel ça répond ?
2. Est-ce le risque le plus élevé actuellement ?
3. Cette solution a-t-elle le meilleur rapport coût/efficacité ?

DICP


Accessibilité
Disponibilité
Confidentialité
Pérennité
Critères de sécurité
Preuve
Intégrité
Traçabilité
Authenticité
Imputabilité
Véracité
Non-répudiation

DICP - DISPONIBILITÉ

- On se protège contre **l'interruption d'un service** pour les personnes qui sont censées pouvoir y accéder (notion associée : **accessibilité**)
  - ressource doit être utilisable en des temps de réponse acceptables
  - en interne : dimensionner correctement (redondance) et gérer efficacement
  - en externe : fournisseurs de service s'engagent à fournir une certaine **continuité de service**
- Mise en place d'une **politique de sauvegarde** (rapport coût/risque)

DICP - INTÉGRITÉ

- On se protège contre **la modification (voire la destruction) non souhaitée d'informations** ⇒ L'information est **authentique et complète**
- On parle donc ici de **protection en écriture**
- Problèmes liés :
  - systèmes d'exploitation & applications
  - transmission des données
  - procédures de sauvegarde
  - hashing & cryptographie

DICP - CONFIDENTIALITÉ

- On se protège contre **la divulgation d'informations** en dehors des personnes autorisées
  - ⇒ Maintien du secret (**non-divulgation**)
- On parle donc ici de **protection en lecture**
- Problèmes liés :
  - contrôle d'accès
  - cryptographie

PRIORISATION DIC

- Il y a toujours un secteur plus critique que les autres en fonction des organisations :
  - **Confidentialité** : pharmaceutiques, publiques
  - **Intégrité** : finances
  - **Disponibilité** : e-commerce
- Il faut **aligner les besoins réels de l'organisation** avec les mesures de sécurité prises

CONTRÔLE DES ACCÈS

- **Identification** : de qui s'agit-il ? (identifiant, *login*…)
- **Authentification** : vérification de cette identité (mot de passe, biométrie, etc.)
- **Autorisations** : qui a le droit de faire quoi ?
- **Contrôle des accès** : rendu possible grâce aux 3 notions précédentes

DICP - PREUVE

- Identification / authentification participent donc à confidentialité + intégrité, mais aussi à la notion de **preuve** :
  - **non-répudiation** : ne pouvoir nier qu'un événement a eu lieu
  - **imputabilité** : attribution d'une action à une entité donnée
  - **traçabilité** : reconstitution des événements à partir de données enregistrées (*logging*)

PREUVE - POUR QUOI FAIRE ?

- Gestion des incidents (reconstitution d'attaque, *forensics*…)
- Analyse des comportements utilisateurs (optimisation)
- Audit (diagnostic de sécurité)
- Systèmes de surveillance (détection d'incidents), IA

APPROCHES DÉFENSIVES

1. Protection uniforme
2. Zones protégées
3. Protection centrée sur l’information
4. Protection orientée sur les vecteurs d’attaque

PROTECTION UNIFORME

- Approche très commune, bon point de départ
- Toutes les parties de l’organisation reçoivent une protection du même type
  - pare-feu, VPN, IDS, antivirus, patching…
- Tous les systèmes sont traités de la même façon
- Limitation : tous les systèmes n’ont pas la même criticité

ZONES PROTÉGÉES

- Créer un environnement très segmenté
- Les « unités de travail » plus critiques sont compartimentées
- Les accès à ces segments critiques sont très restreints
- Mise en place de pare-feux internes + VLANs / ACLs
- Les zones protégées **n'empêchent pas les brèches externes** : elles contrôlent les dommages internes

PROTECTION CENTRÉE SUR L'INFORMATION

- Identification des ressources critiques et protection par couches
  - les données sont accessibles par les applications
  - les applications résident sur des hôtes
  - les hôtes communiquent par les réseaux
- Idée : les contrôles d'accès « accompagnent » les données, peu importe où elles sont utilisées
- Approche extensible (s'adapte à la quantité, à la répartition et au flux des données)

PROTECTION ORIENTÉE VECTEURS D'ATTAQUE

- La menace a besoin d'un **vecteur** pour atteindre la vulnérabilité
- Principe : empêcher la menace d'utiliser le vecteur
- Exemples de vecteurs et de mesures associées :
  - clé USB ⇒ désactiver USB
  - pièces jointes email ⇒ bloquer ou scanner
  - usurpation d'email ⇒ vérifier l'adresse IP auprès du serveur

RÉPARATION APRÈS INCIDENT

- Se contenter de *fix* les problèmes détectés : pas efficace
  - car alors on traite les symptômes, pas la maladie
- Compromission ⇒ *backdoors* et autres malwares potentiels
- Quand c'est possible, bonne stratégie : **tout réinstaller de zéro**

FACT

On ne peut pas protéger ce qu'on ne connaît pas

GESTION DE CONFIGURATION

- On ne peut pas gérer les vulnérabilités sans connaître le Système d'Informations
- Comme pour la détection d'intrusion, on va vouloir « détecter » et gérer les modifications du système
- **Gestion de configuration** :
  - description technique du SI (logiciels, matériel, doc…) ⇒ document de base
  - modifications qui sont faites au fil du temps ? ⇒ modification du document de base

RÉSUMÉ

- **100 % sécurité n’existe pas**
  - par nature, les solutions préventives ne suffisent pas
  - la détection **doit** venir en soutien
  - tout est question de **gestion de risques**
  - sans rentrer en conflit avec les processus métier
- Flux **entrants** / **Prévention**, Flux **sortants** / **Détection**
- **DIC + P**
- Différentes approches défensives, non mutuellement exclusives