

# Module Cyber Sécurité

## Notion de risque

Jean-Marc MULLER

Sébastien SCHMITT



## Critères DIC

- Besoins de sécurité ? Pour garantir quoi ?

→ Utilisation de 3 critères D.I.C.

➔ Disponibilité

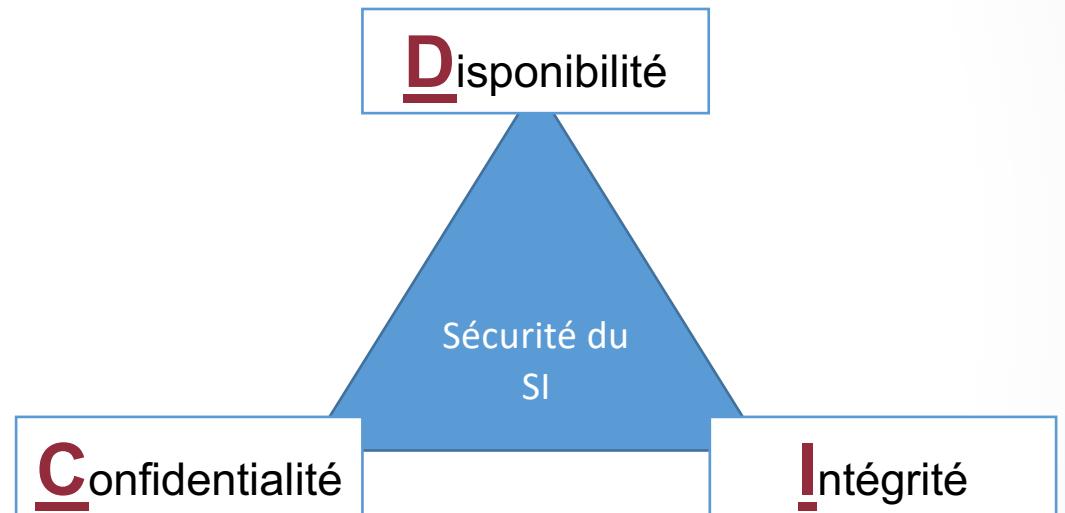
    ⇒ Accessibilité de la ressource

➔ Intégrité

    ⇒ Information confirme aux attentes  
    ⇒ Information non altérée

➔ Confidentialité

    ⇒ Information accessible aux seuls ayant droits



## Critères DIC

- Besoins de sécurité ? Pour garantir quoi ?

→ "Preuve"

Preuve

- Critère complémentaire au D.I.C.
- Contrôler les circonstances selon lesquelles un bien évolue
  - Notion de **träçabilité** des actions menées
  - Notion d'**authentification** des utilisateurs afin de pouvoir mener une action
    - Notion d'**imputabilité** au responsable de l'action
- Obligatoire dans certains domaines critiques
  - Bancaire
  - Énergétique
  - Militaire

## Critères DIC

- Évaluation des critères DIC(P) afin d'assurer le niveau de sécurité adéquat

→ Objectif

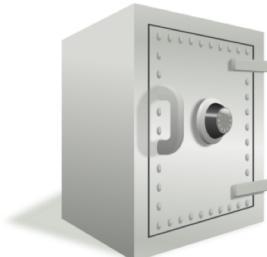
→ Déterminer le niveau DIC(P) d'un bien (élément d'un système d'information)

→ Comment ?

→ Etablir une échelle pour chaque critère

→ Déterminer le niveau du bien dans chaque critère

→ Exemple :



Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Aucun
Niveau de Preuve du bien	Faible



Un bien doit bénéficier de mesures de sécurité adaptées à son DIC(P)

## Définition d'un risque

- Les critères DIC(P) d'un bien peuvent être dégradés par un RISQUE

### → Description d'un risque

$$\text{RISQUE} = \text{Menace} * \text{Vulnérabilité} * \text{Impact}$$

#### → Menace

→ Attaque possible du bien par un élément perturbateur

#### → Vulnérabilité

→ Faiblesses ou failles connues ou inconnues d'un bien (Humaine, Réseau, Système ...)

#### → Impact

→ Conséquence de l'occurrence du risque

→ Financier, Réputation, Continuité d'activité, Judiciaire..

→ Conséquence de dégradation des critères DIC(P)

### → Mesure d'un risque

→ RISQUE = Probabilité d'occurrence \* Gravité

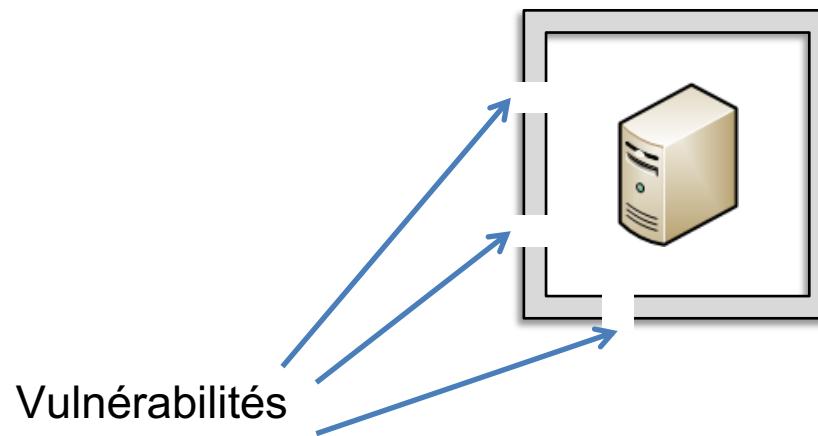
→ D'autres formules possibles

## Les vulnérabilités

- Vulnérabilité

→ Faiblesse, fragilité d'un élément du SI

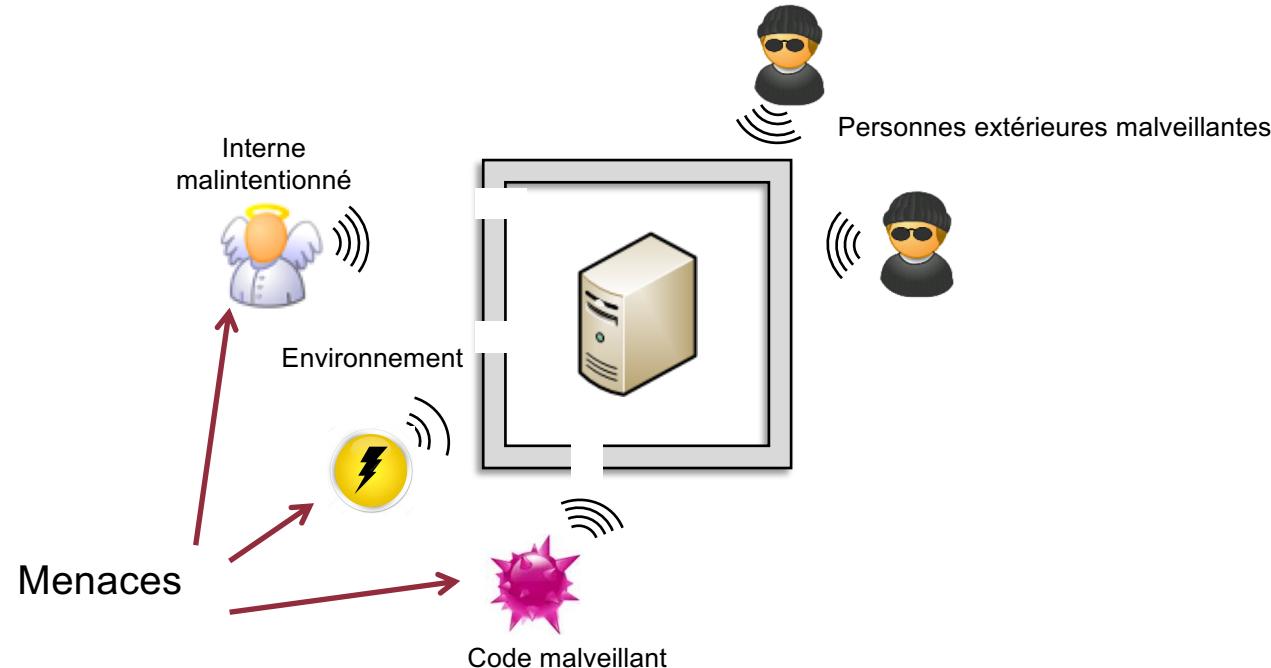
- ➔ Au niveau de sa conception
- ➔ Au niveau de sa réalisation
- ➔ Au niveau de sa configuration
- ➔ Au niveau de son utilisation



## Les menaces

- Menace

→ Cause potentielle d'incident pouvant entraîner un dommage



## Mesures de sécurité

- Différentes façons pour définir les mesures de sécurité permettant de réduire les risques
  - Se baser sur le bon sens
    - ➔ Choix subjectif, difficile à justifier
    - ➔ Très rapide à produire
  - Choix de mesures selon les bonnes pratiques
    - ➔ Ensemble de mesures types à appliquer par défaut sans réfléchir
    - ➔ Choix guidé
    - ➔ Approche rapide
  - Choix des mesures selon une méthodologie établie
    - ➔ Évaluer les risques au regard de chaque critère de sécurité à maintenir (analyse de risques)
      - ➡ ISO27005 (gestion des risques)
    - ➔ Réduire les risques menaçant le système d'information en se basant sur des bases de connaissances
      - ➡ ISO27002 (mesures de sécurité), IT-Grundsatz-Kataloge version 2015 (anglais)
    - ➔ Approche plus lente
    - ➔ Plus précise et légitime pour les décideurs (possibilité de certification)

## Mesures de sécurité

- Différence entre sûreté et sécurité

→ Sûreté

- Protection contre les dysfonctionnements et **accidents involontaires**
  - Exemples:
    - Coupe électrique
    - Panne disque
- Prévisible
  - Opération de maintenance préventive
- Quantifiable statistiquement

→ Sécurité

- Protection contre les **actions malveillantes volontaires**
  - Exemples:
    - Déni de service
    - Vol d'information
- Non quantifiable
- Possibilité d'**évaluation du risque**

## Mesures de sécurité

- Différence entre sûreté et sécurité

- **Sûreté**

- Ensemble des mécanismes mis en place pour assurer la continuité de fonctionnement du système d'information au niveau de DIC(P) attendu

- **Sécurité**

- Ensemble des mécanismes destinés à protéger le système d'information des utilisateurs ou processus n'ayant pas l'autorisation de le manipuler et susceptibles de dégrader les critères DIC(P)