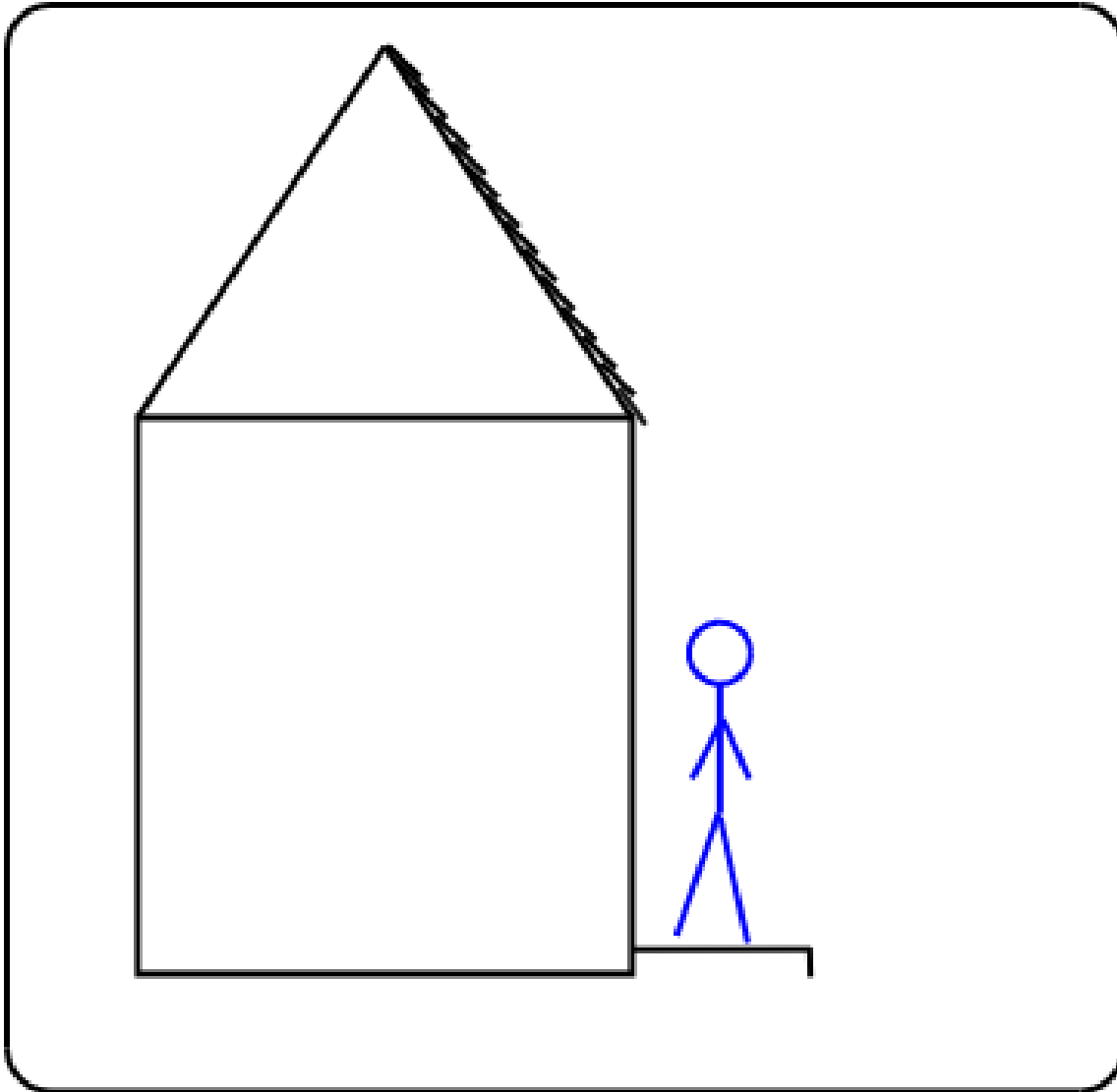


GR - Introduction

UNIV-PAU / LP

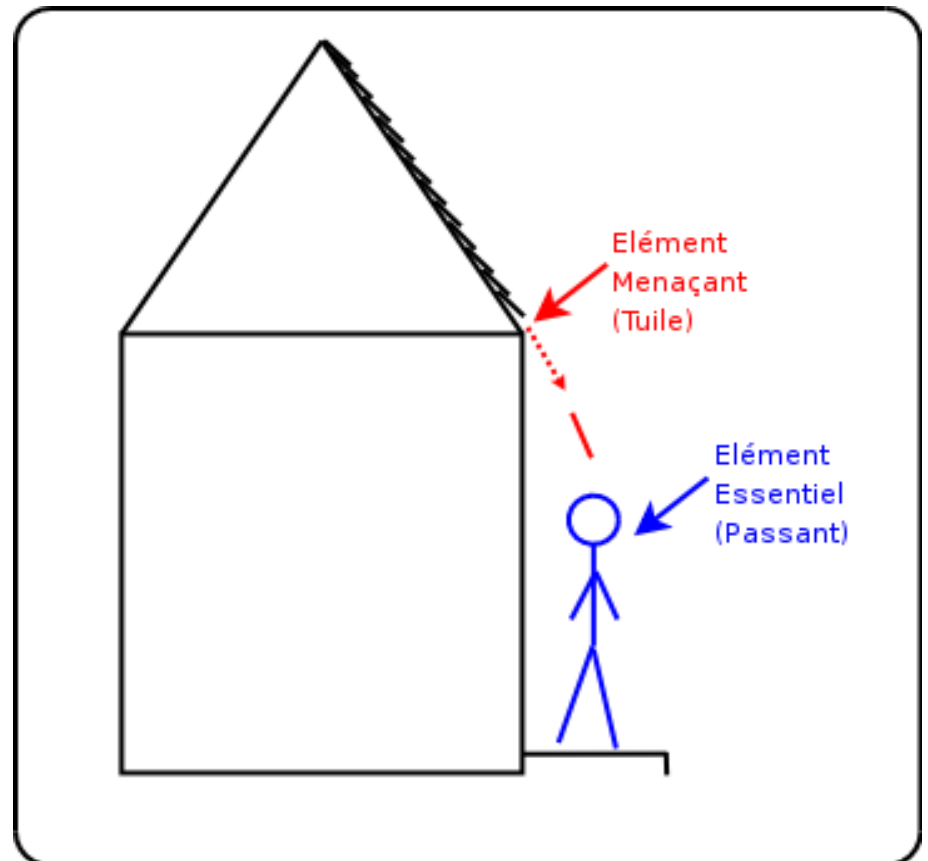
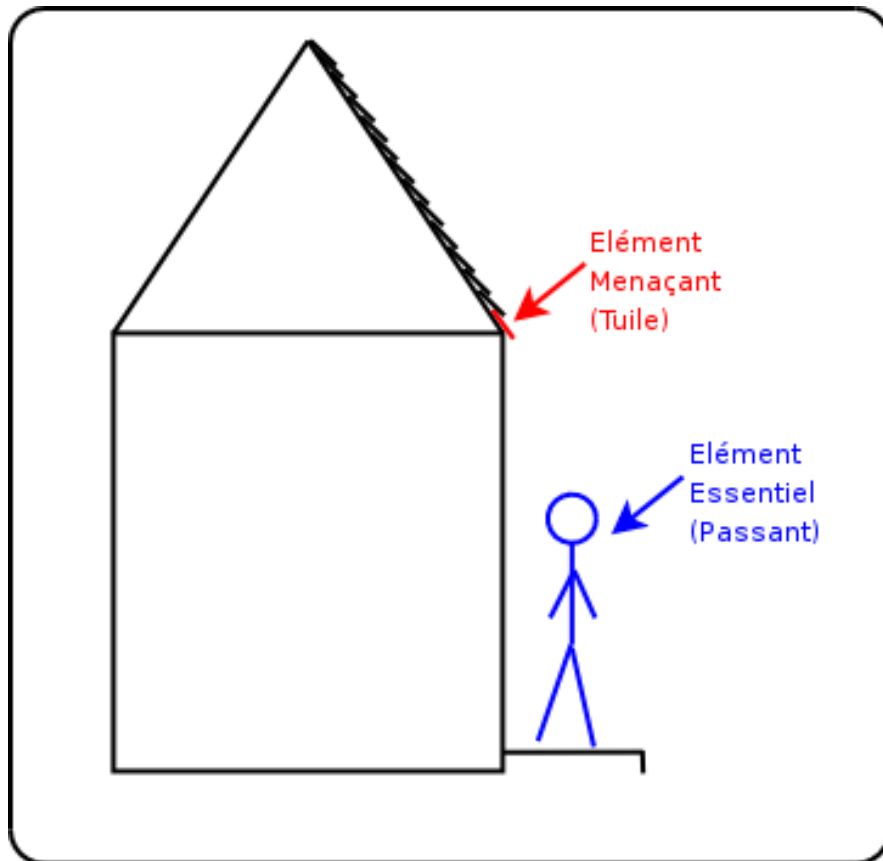
Introduction à la gestion du risque

Fait divers

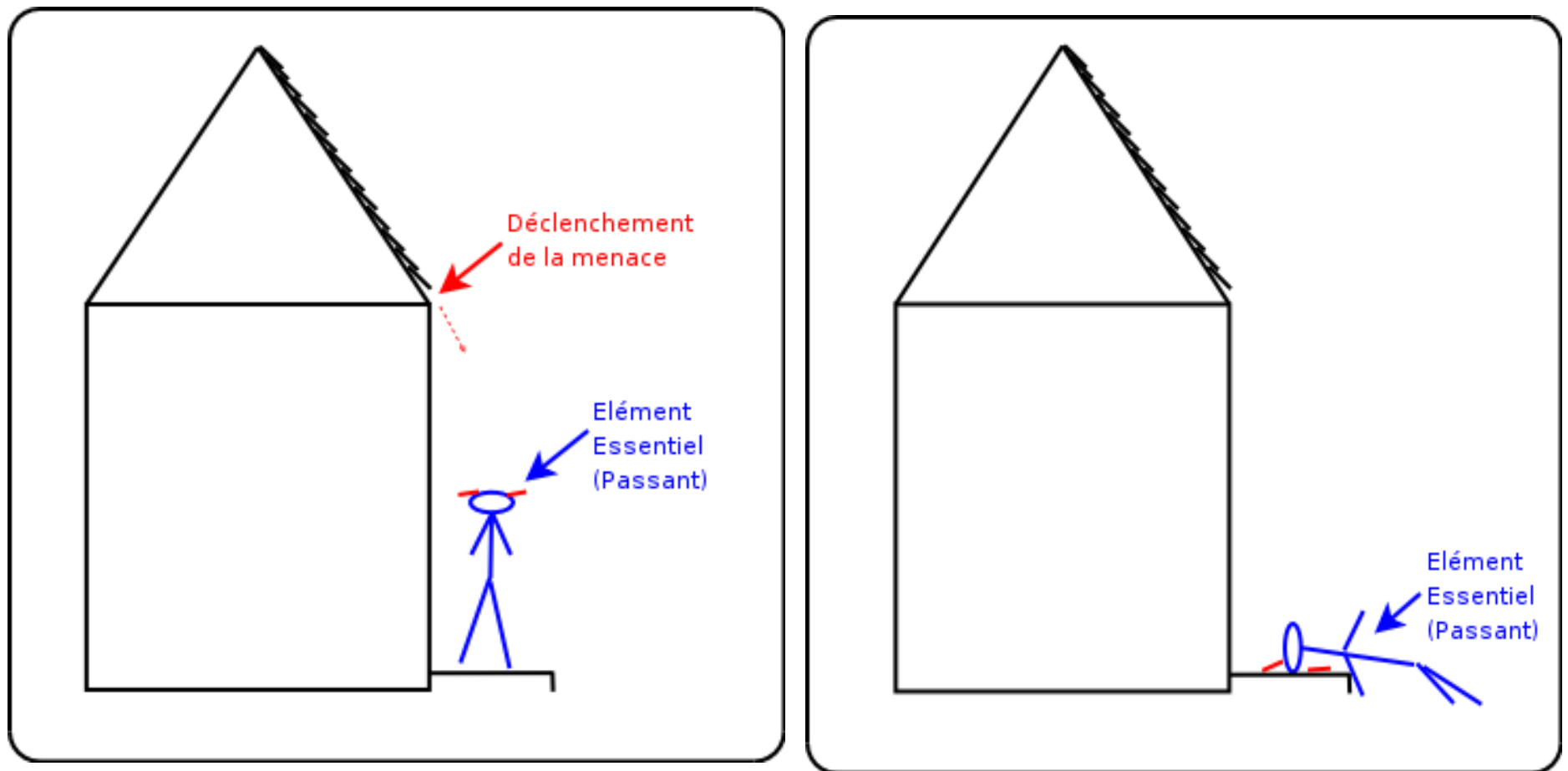


- Un passant se promène en ville sur un trottoir.

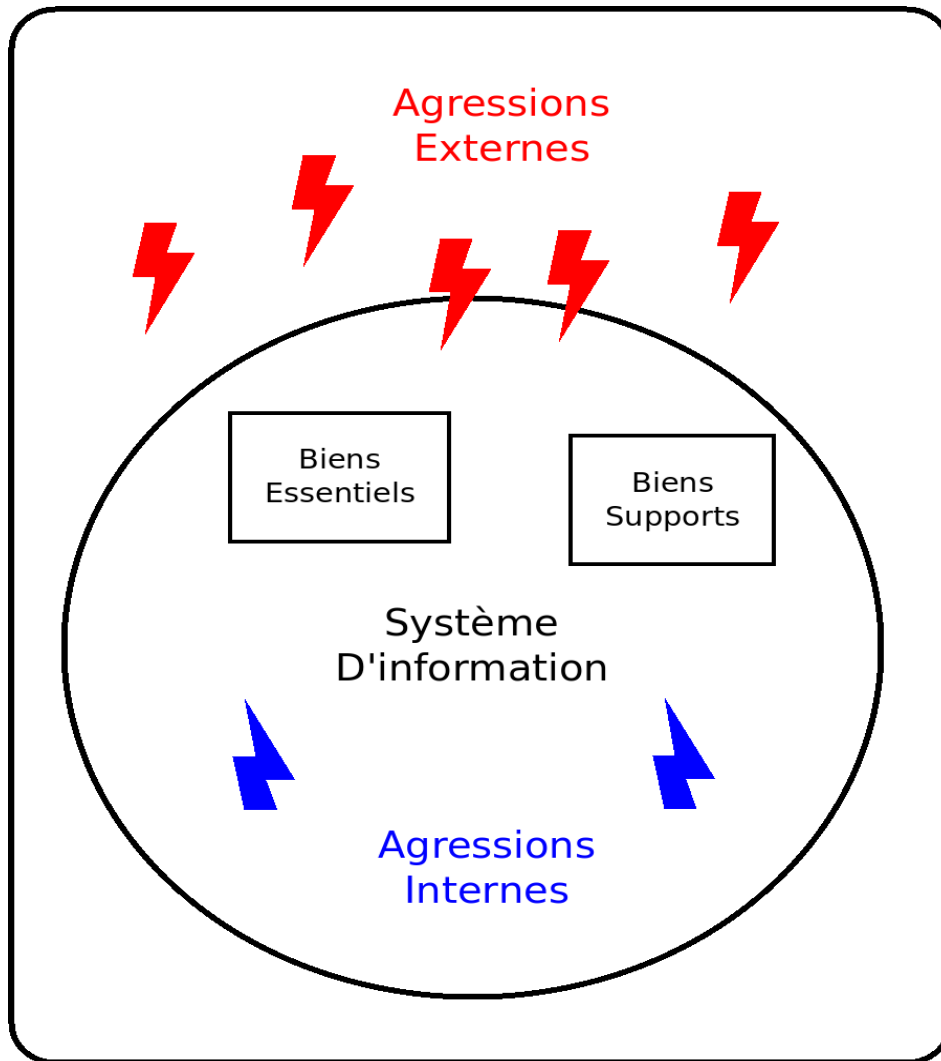
Fait divers



Fait divers



Le système d'information



- Le SI est exposé à des éléments menaçants et est soumis à des agressions.
 - Internes
 - Externes
- Exemples d'agressions internes :
 - Panne de matériel
 - Erreur de manipulation d'un exploitant
 - Malveillance interne
- Exemples d'agressions externes :
 - Succès d'une application entraînant une saturation des lignes
 - Attaque d'un pirate

Expression des besoins de sécurité

- Disponibilité

- Propriété d'accessibilité au moment voulu des biens essentiels par les utilisateurs autorisés

- Intégrité

- Propriété d'exactitude et de complétude des biens essentiels

- Confidentialité

- Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.

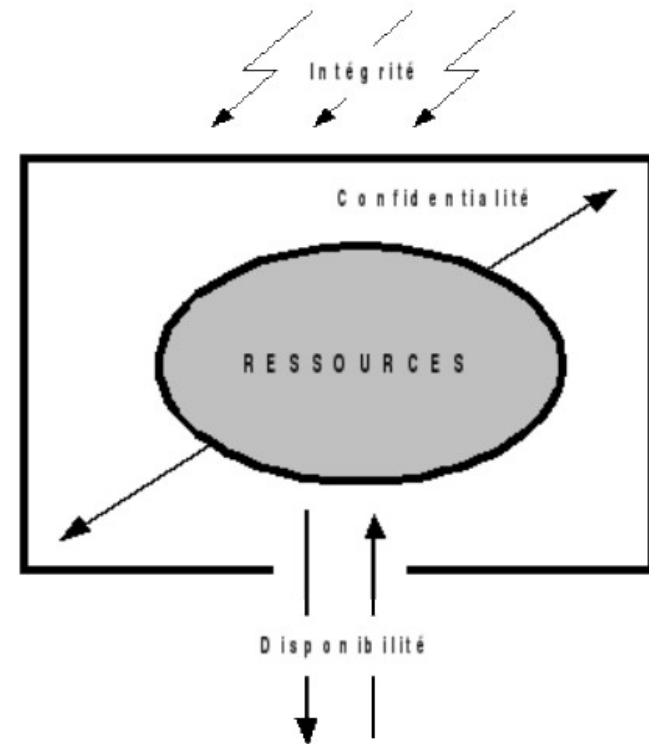
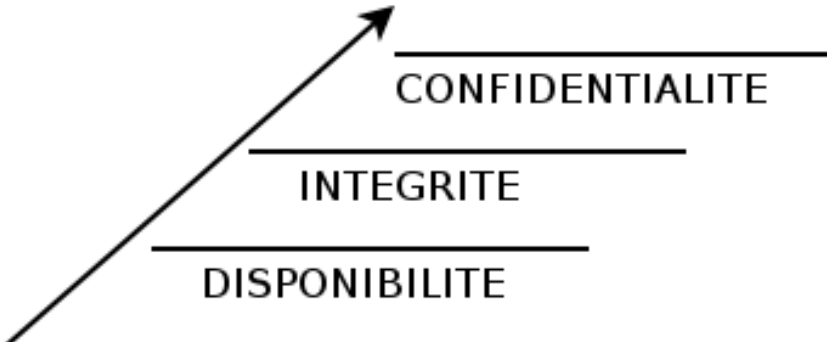
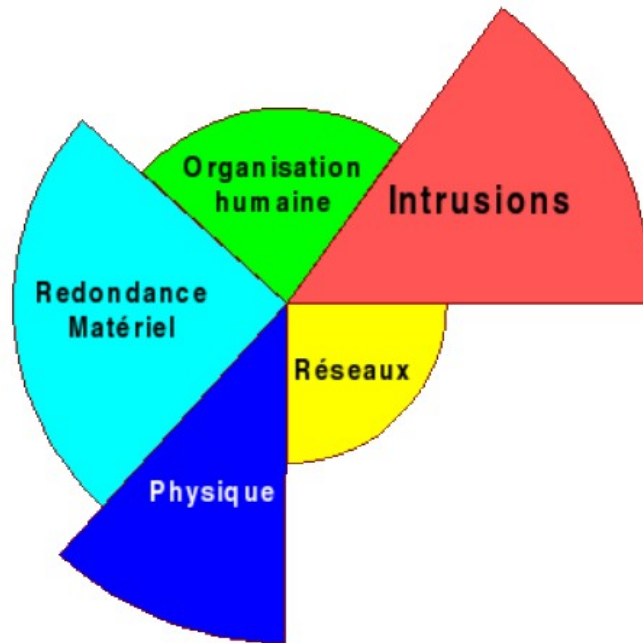


Tableau récapitulatif



	Organisation Humaine	Logiciel Machine	Physique
Prévention			
Détection			
Réaction			

Homogénéité dans les investissements

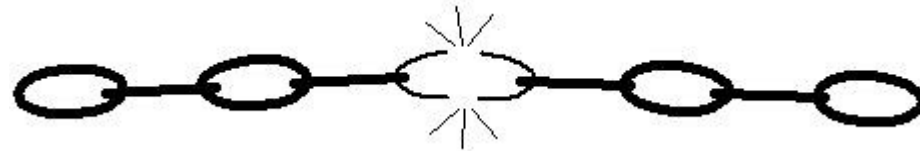


NON



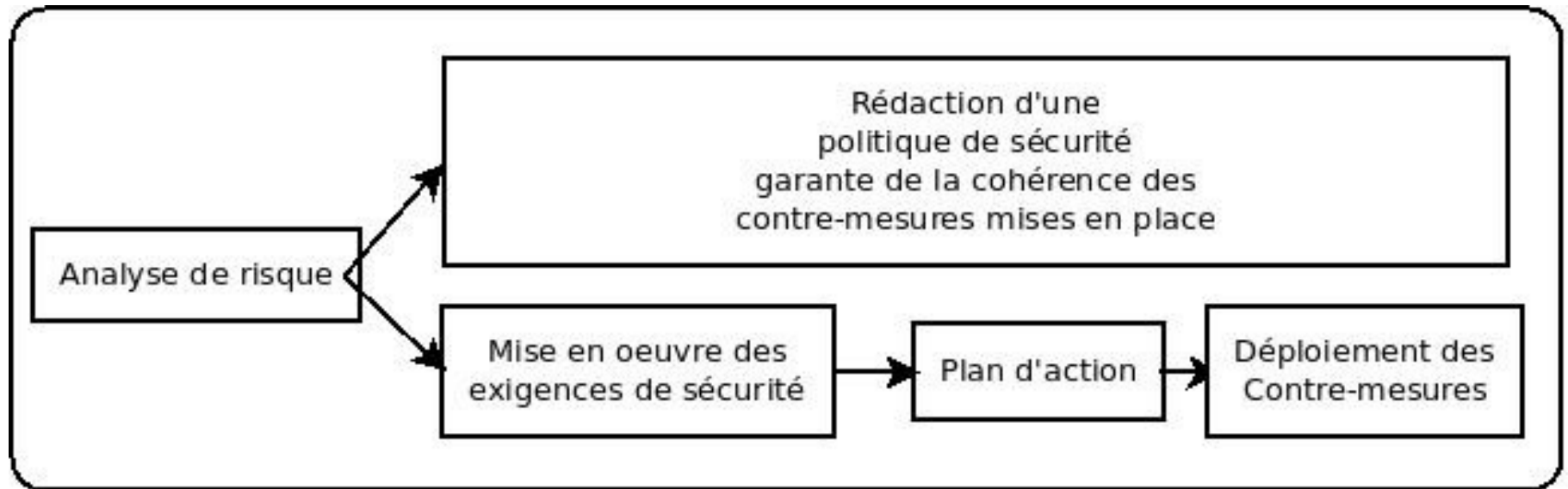
OUI

Maillon faible

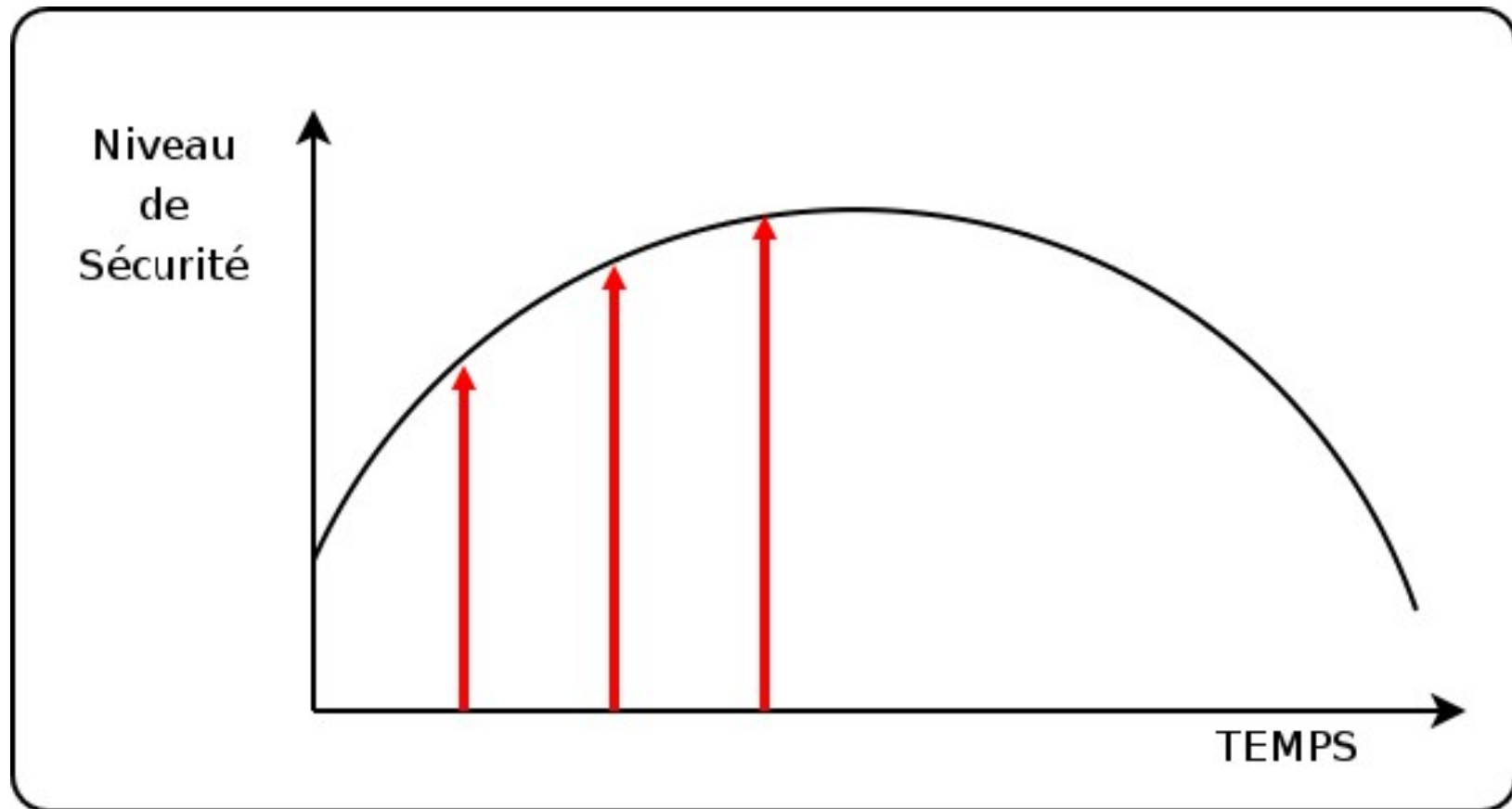


Le niveau de sécurité global est toujours égal à celui
du maillon le plus faible

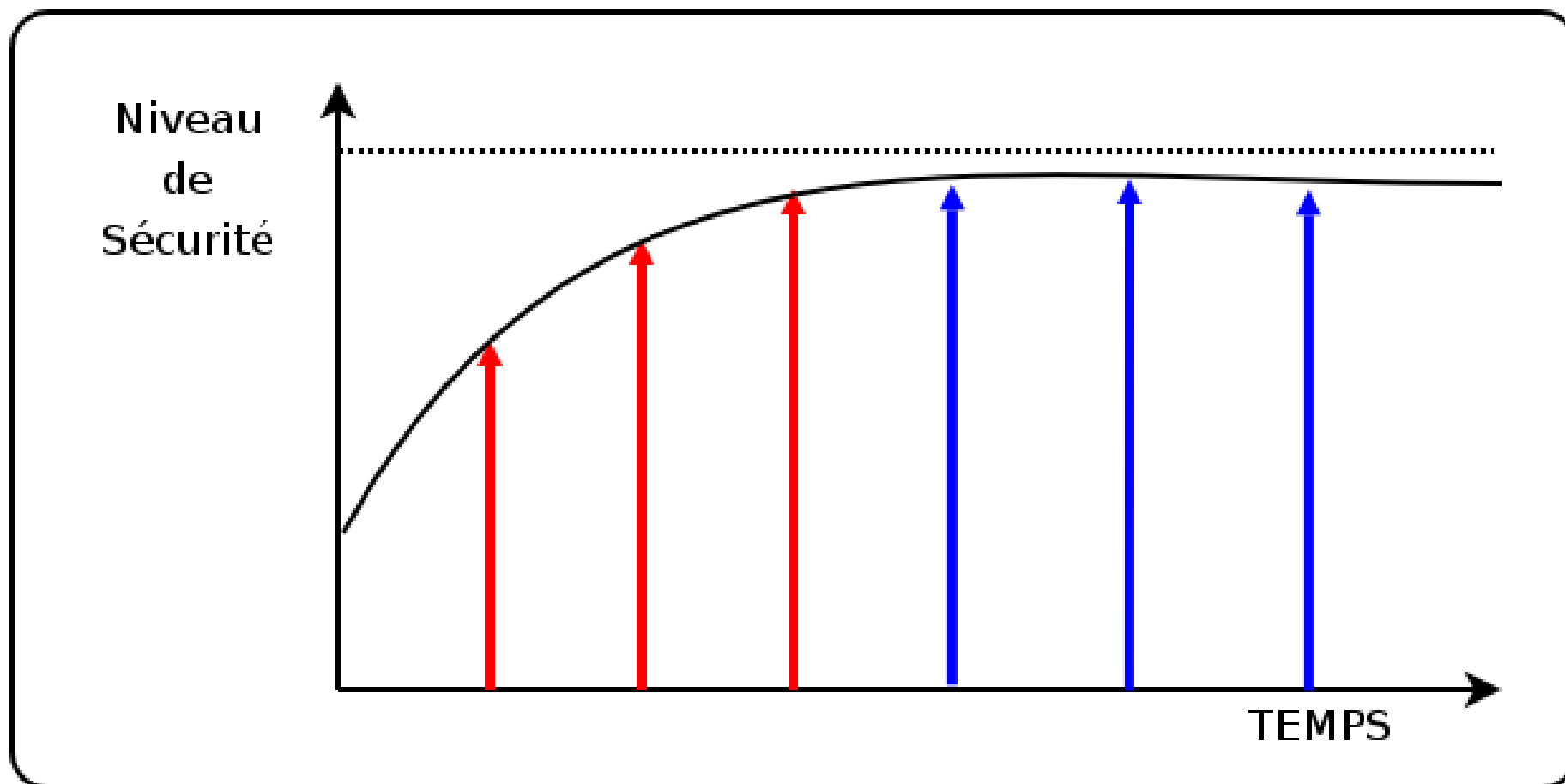
Acquérir un niveau de sécurité



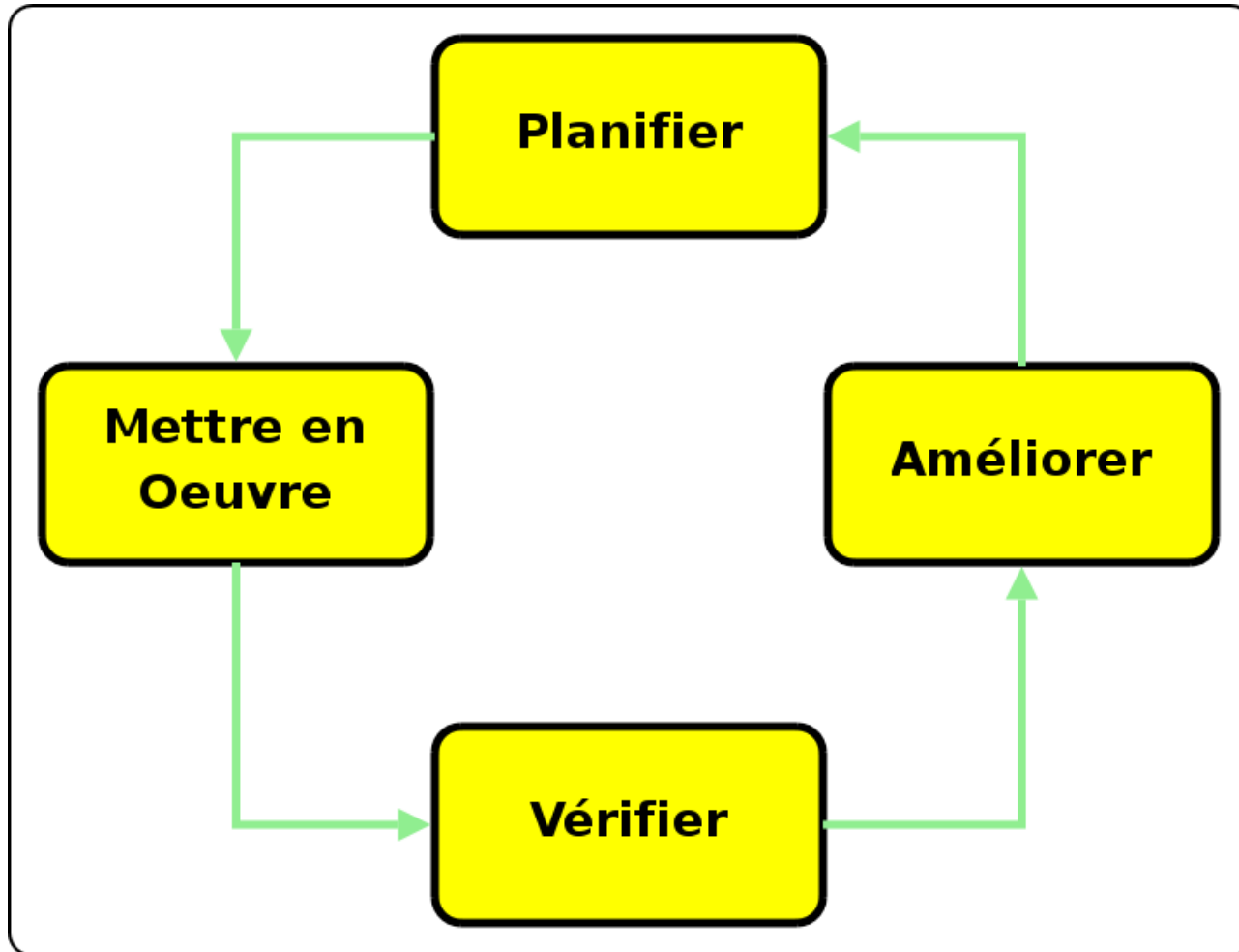
Maintenir un niveau de sécurité



Maintenir un niveau de sécurité

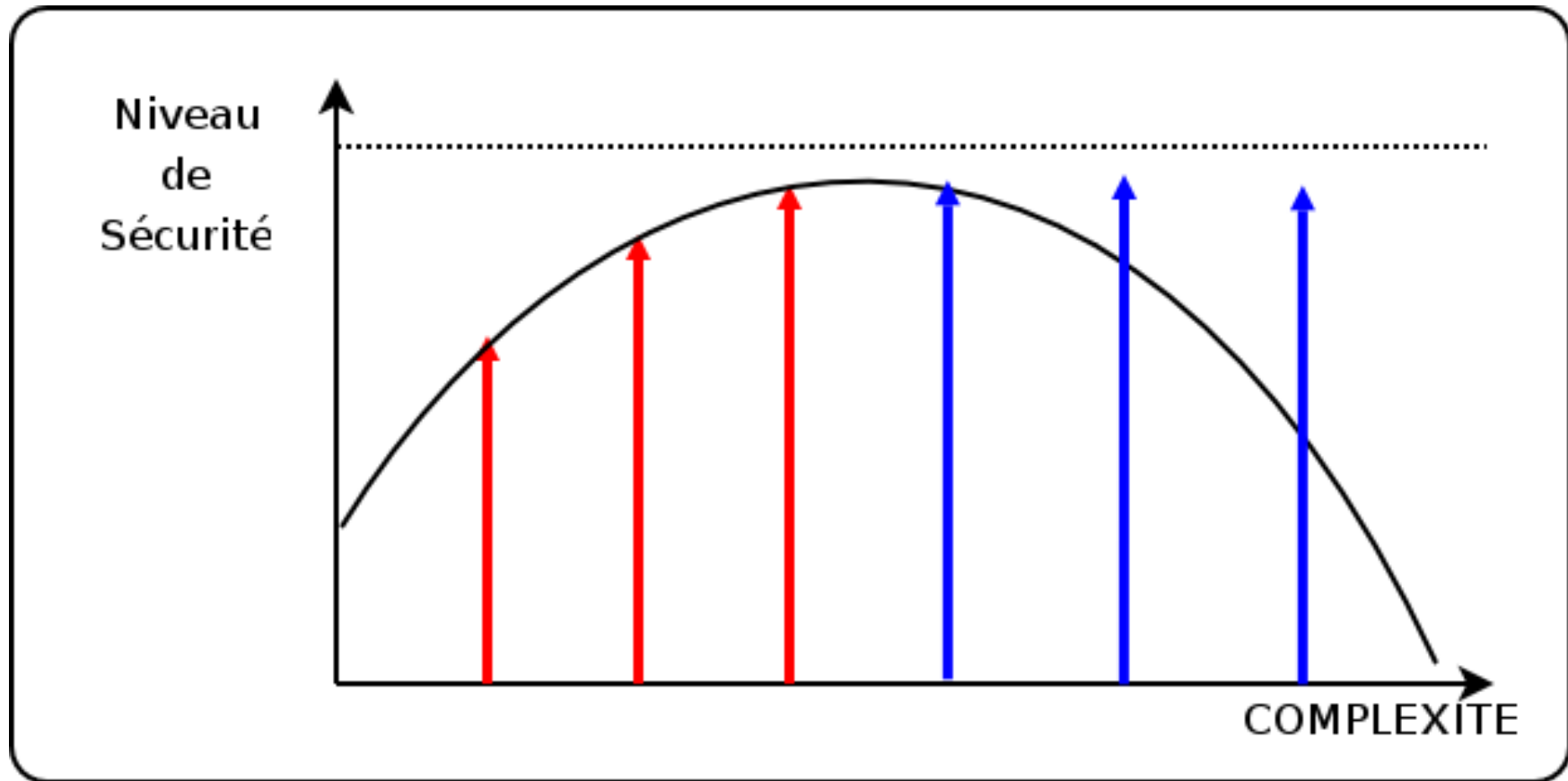


PDCA



- La norme ISO 27001 est basée sur la mise en place d'un système de management du type PDCA (roue de Deming)
- L'objectif du SMSI est d'atteindre le niveau de sécurité nécessaire et surtout de s'y maintenir
- Réalisation de tableaux de bord SSI

Maintenir un niveau de sécurité



Les dangers de la complexité

Quelques grands principes

- La nécessité d'une approche globale
- Le principe du moindre privilège
 - Tout ce qui n'est pas explicitement autorisé est interdit
- Le principe de la défense par couche (défense en profondeur)
 - Les ressources sont protégées à tous les niveaux où il est possible d'agir. En cas de compromission sur un des niveaux, des protections de natures différentes sont en mesure d'arrêter une attaque.
- Les logs et la supervision (le "pouls" du SI en temps réel)
 - Surveillance long terme / court terme
 - Être proactif

Quelques grands principes

- La "non-sécurité" par l'obscurité
 - Exemple : Un éditeur qui ne dévoilerait pas les failles de sécurité dans son logiciel.
- Le principe de lenteur
- Bon sens et Modestie