



Université Assane Seck de Ziguinchor
UFR Sciences & Technologies
Département d'Informatique

Chapitre 2 ●

Généralités sur la ●

Sécurité Informatique ●

● ● ●

Approche traditionnelle

De la sécurité informatique

 La sécurité c'est la:

 Prévention

 Détection

 Réaction

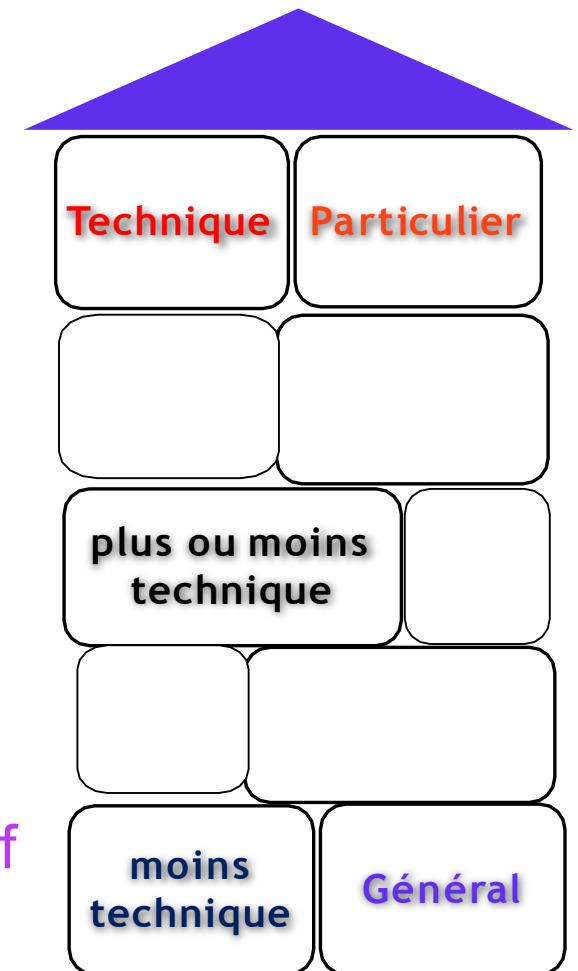
Approche d'étude pour aborder la cybersécurité

👉 Les risques

- ✓ Vulnérabilités
- ✓ Menaces
- ✓ Les attaques

👉 Les mesures

- ✓ Services ou objectifs ou propriété de sécurité
- ✓ Les mécanismes de sécurité pour atteindre les objectif



Les risques

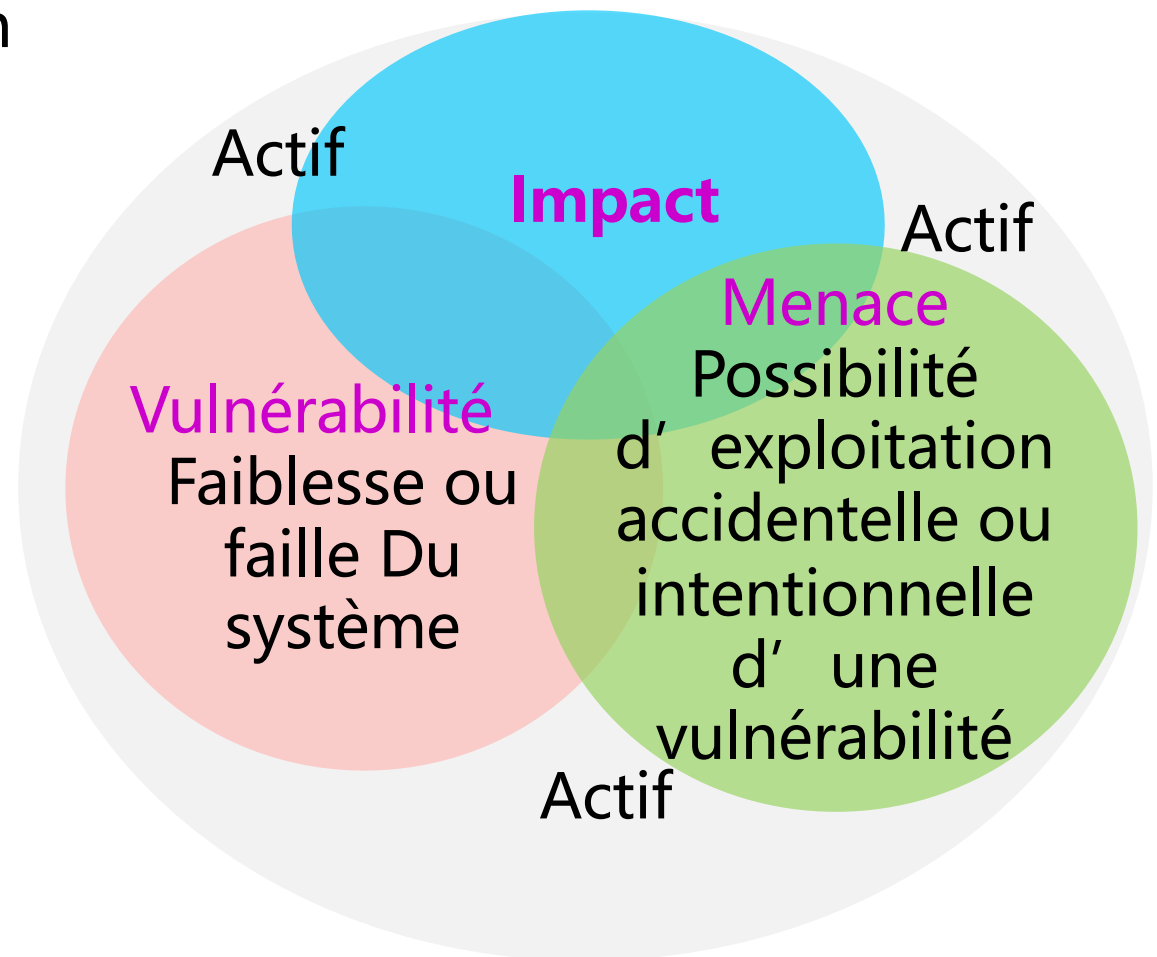
Vulnérabilités, menaces, attaques

Risque: couple (menace, vulnérabilité) qui impacte sur l'information

Menace: est la possibilité qu'un événement nuisible, tel qu'une attaque survienne.

Vulnérabilité: est une faiblesse qui expose un système à une attaque.

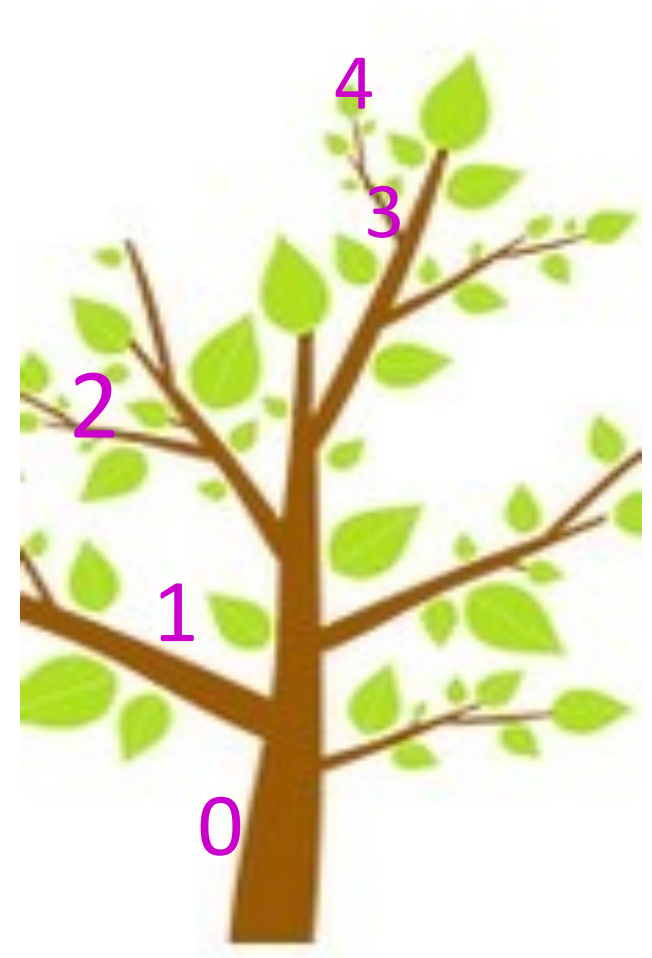
Attaque: est l'exploitation délibérée d'une faiblesse découverte dans un système informatique



Les risques nature des vulnérabilités

- Exemple: on se fixe comme objectif de grimper sur l' arbre
- **Vulnérabilité**: fragilité des branches
- **Menace**: tomber
- **Risque**: se casser un membre ou succomber à ses blessures

- 0**: **Vulnérabilité**=faible, **menace**=tomber,
Risque=presque néant
- 1**: **Vulnérabilité**= peu, **menace**=tomber,
Risque=se casser le bras
- 3**: **Vulnérabilité**= moyen, **menace**=tomber,
Risque=se casser les bras ou jambes
- 5**: **Vulnérabilité** = trop, **menace**=tomber,
Risque= mourir



Les risques

Analyse et gestion

En quatre étapes

- Identifier le risque
- Evaluer le Risque
- Apporter une réponse face au risque
- Suivre le risque

Les risques

Analyse et gestion

- 1. Identifier les risques: faire un brainstorming avec les membres de l'équipe et établir un check liste qui comprend un certain nombre de risques
 - Risques techniques
 - Risques humains
 - Risques fournisseurs
 - Etc....

Les risques

nature des vulnérabilités

- Physiques



- Technologique



- Logicielle d'application



- Protocole de communication



- Vulnérabilité des acteurs



Les risques

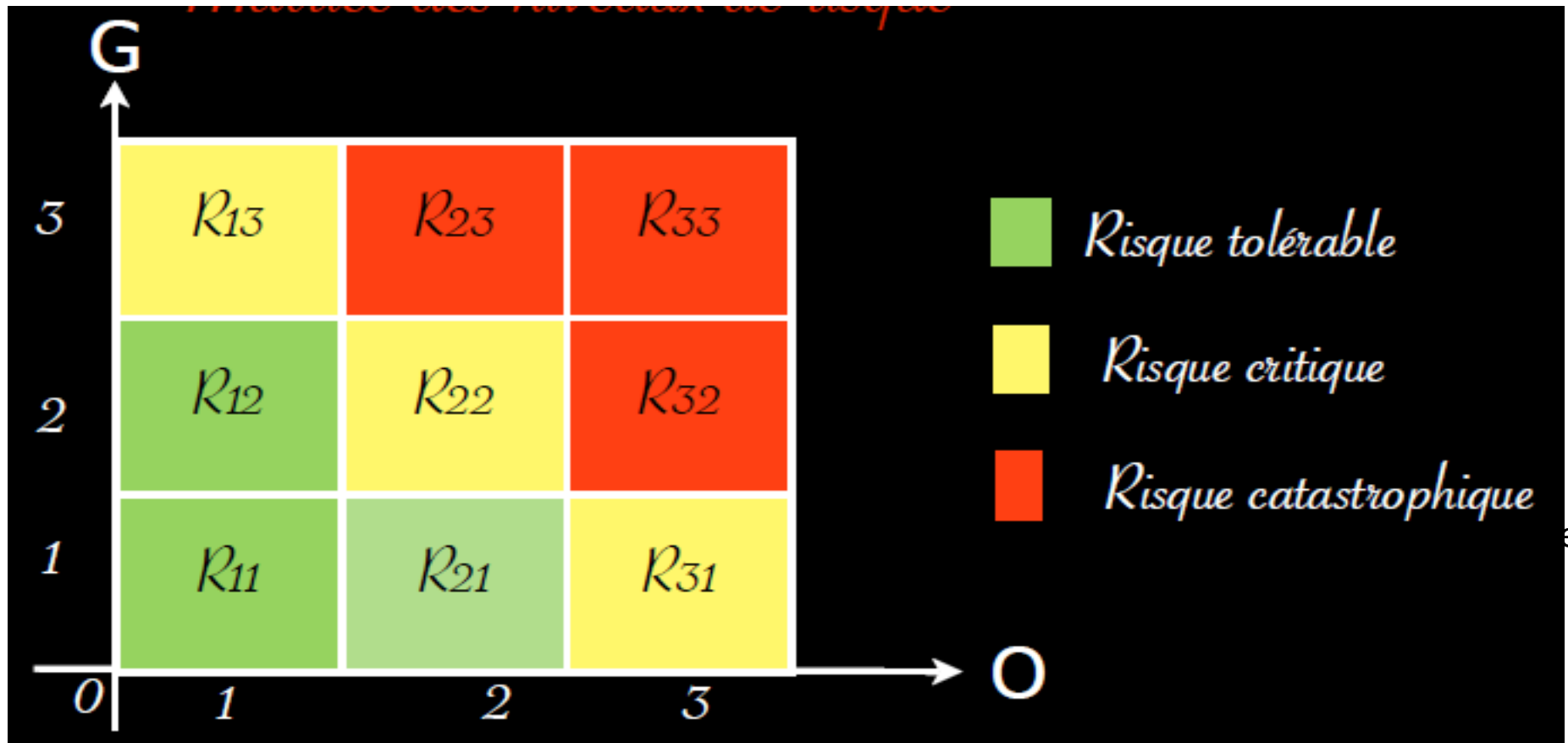
Analyse et gestion

- 2. Evaluer le risque: quantifier, chiffrer le risque avec des valeurs
 - Paramètres de quantification
 - Occurrence O = la probabilité que le risque se produise
 - Gravité G = l'impact du risque sur le système
 - Criticité $C : O \times G$
 - Exemples de valeurs de C , fonction de O et G
 - faible = 1, moyenne=2, forte=3

Les risques

Analyse et gestion

- Matrice des niveaux de risque:



Pour le risque R_{13} , même s'il est improbable, sa gravité quand il se produit est forte: on peut le mettre dans la zone rouge

Les risques

Analyse et gestion

- 3. Apporter une réponse face au risque
 - Si le risque est fort mener les plan d' action suivantes:
 - Action 1- éviter le risque (réduire O)=Prévention
 - Action 2- atténuer le risque (réduire G)= Protection
 - Action 3- transférer le risque: l'externalyser , i.e transférer vers une entreprise plus compétente ou l'assurer
 - Action 4: gérer le risque = Provision (disposer de provision permettant d'absorber le risque)

Les risques

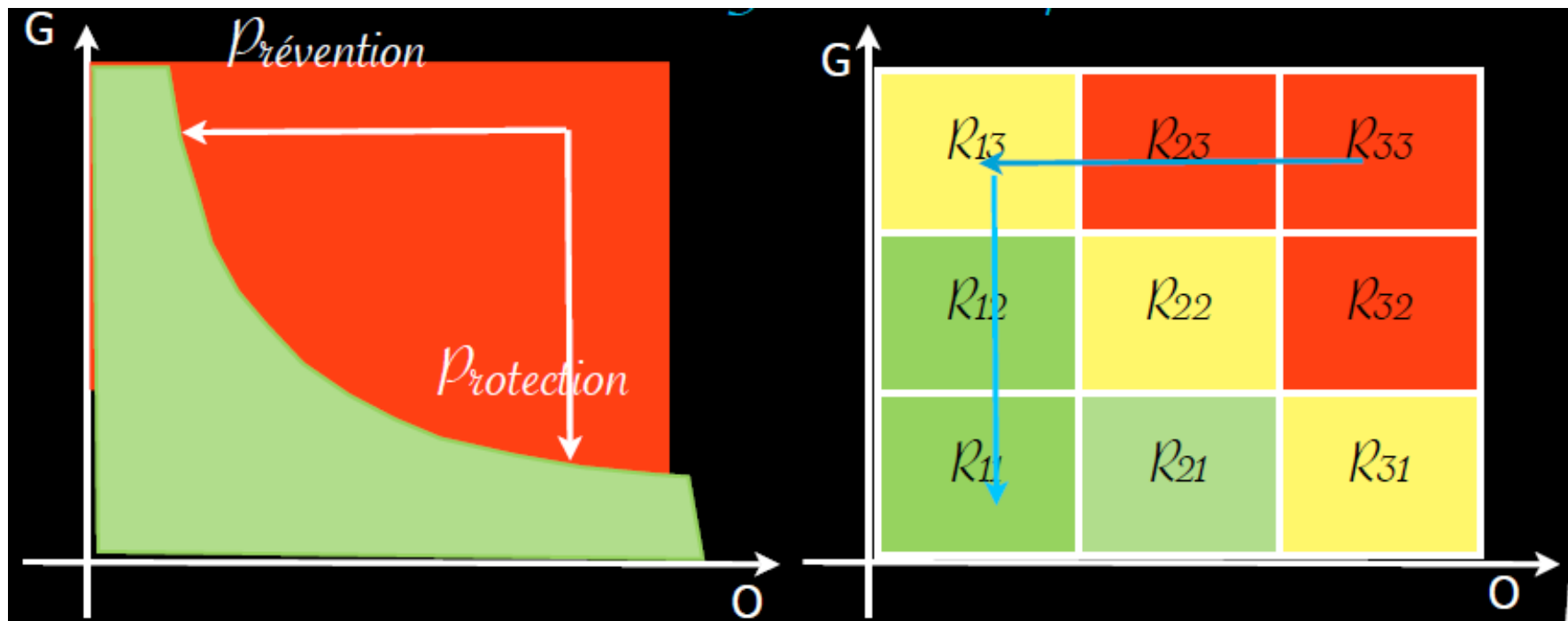
Analyse et gestion

- 4. Suivre les risque: pouvoir identifier l' état dans lequel est le risque,
 - Supprimer les risques passés
 - Surveiller les risque actifs
 - Surveiller les risque latent (futurs)
- Deux stratégies pour suivre les risques
 - Réduire la Probabilité (-O) = plan de prévention
 - Réduire la gravité(-G)= plan de protection
 - Prévention + Protection = Gestion des risques

Les risques

Analyse et gestion

- 4. Suivre les risque
 - Prévention + Protection = Gestion des risques



Prévention + Protection

R33 => **R11**

Les risques

Analyse et gestion

● 4. Suivre les risque

- Tableau de bord pour le suivi des risque

<i>Risques</i>	<i>O</i>	<i>G</i>	<i>C</i>	<i>Plan d'action</i>	<i>O'</i>	<i>G'</i>	<i>C'</i>
<i>R₁</i>	2	3	6	<i>Prévention+Protection</i>	1	2	2
<i>R₂</i>	3	3	9	<i>Prévention+Protection</i>	2	1	2
<i>R₃</i>	2	1	2	<i>Néant</i>	2	1	2
<i>Explosion globale=</i>			17				6

Explosion globale est passe de **17** à **6**

Les risques

Gestion des risques: ISO/IEC 27005

- Gestion des risques liés à la sécurité de l'information
- Le modèle ISO/CEI est aux professionnels de la cybersécurité ce que le modèle de réseau OSI est aux ingénieurs de réseaux.
- Les deux proposent un cadre permettant de cerner et de gérer les tâches complexes.
- La gestion des risques est une discipline pratiquée depuis fort longtemps dans l'industrie ou l'assurance.
 - Dans le domaine de la sécurité de l'information ISO 27005 marque un changement majeur en facilitant la gestion des risques
 - ISO 27005 adopte le modèle d'amélioration continue (PDCA)

Les risques

Gestion des risques: ISO/IEC 27005

National Institute of Standard and Technology (**NIST SP 800-30**) (for U/S government sector)

ISO/IEC 27005

OCTAVE Published by Software Engineering Institute of Carnegie Mellon University in 1999

IRAM

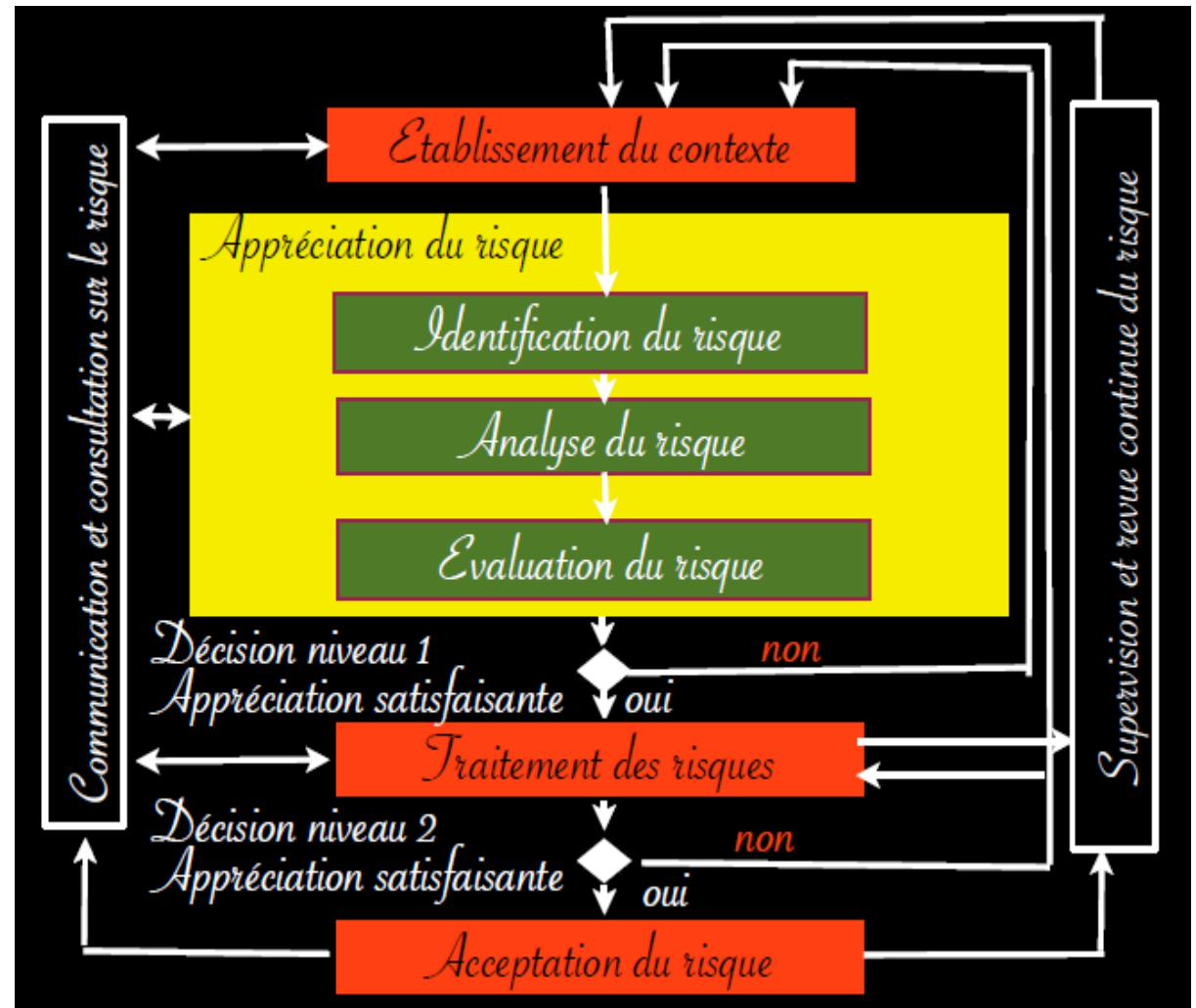
EBIOS originally launched by French government, but it now supported by a team

of experts of diverse origins

CRAMM (A risk analysis method developed by the Central

Communication and Telecommunication Agency, a British government organisation

MEHARI: en France par CLUSIF



Les risques

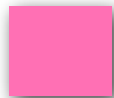
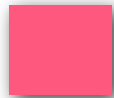
quelques vulnérabilités

- Infrastructure inadéquate
- Sécurité physique insuffisante
- Réseaux connectés à internet
- Transmission sans fil
- Erreur logicielle,
- Négligence (mot de passe volé)
- Manque d'éthique, erreurs humaines



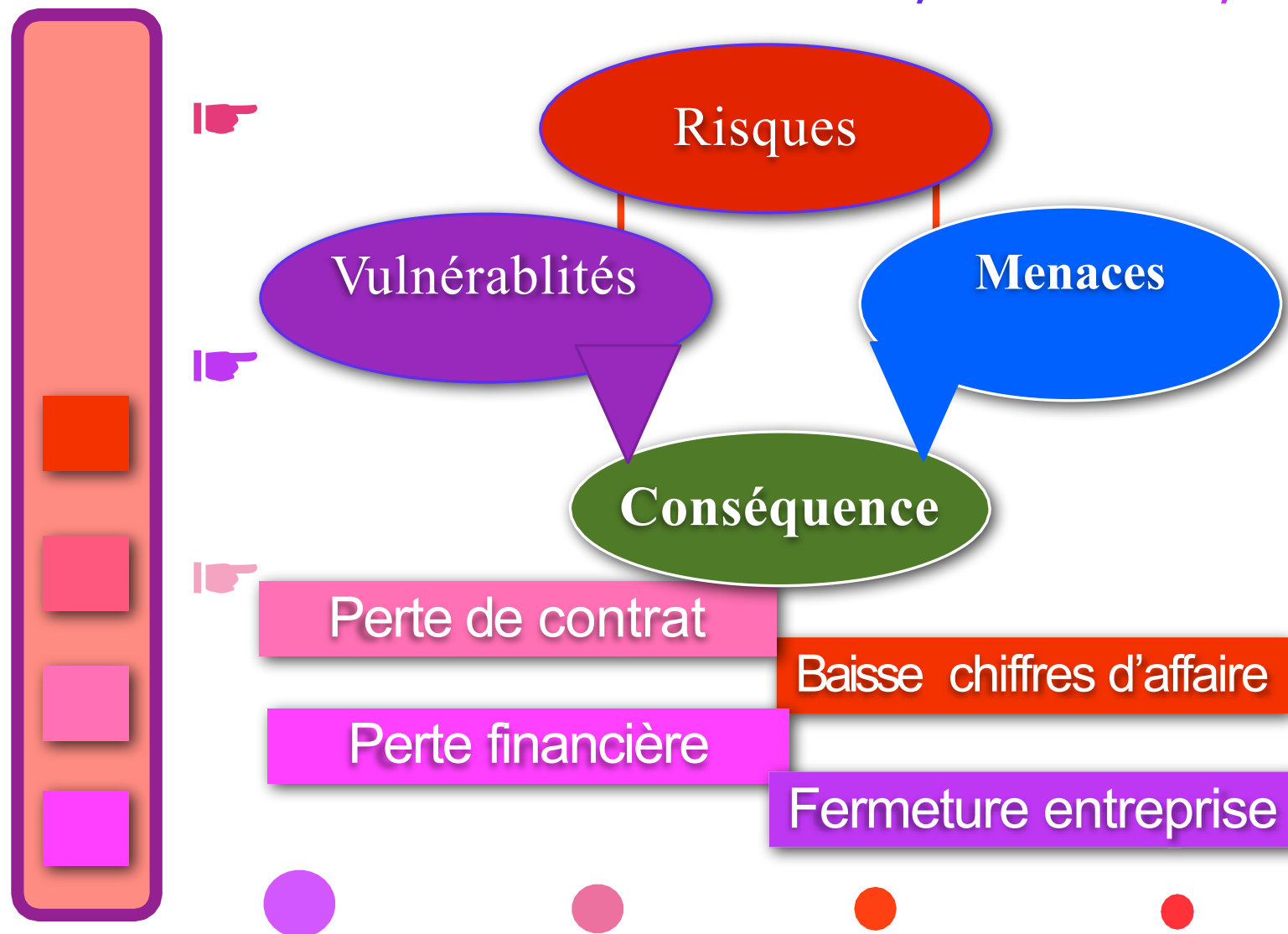
Les risques origine des menaces

- Catastrophe naturelle
- Terrorisme, vol..
- Internet (pirate, virus)
- Interception de trafic
- Virus, hacker
- Vol de données confidentielles (mot de passe ..)
- Comportement malicieux.



Les risques

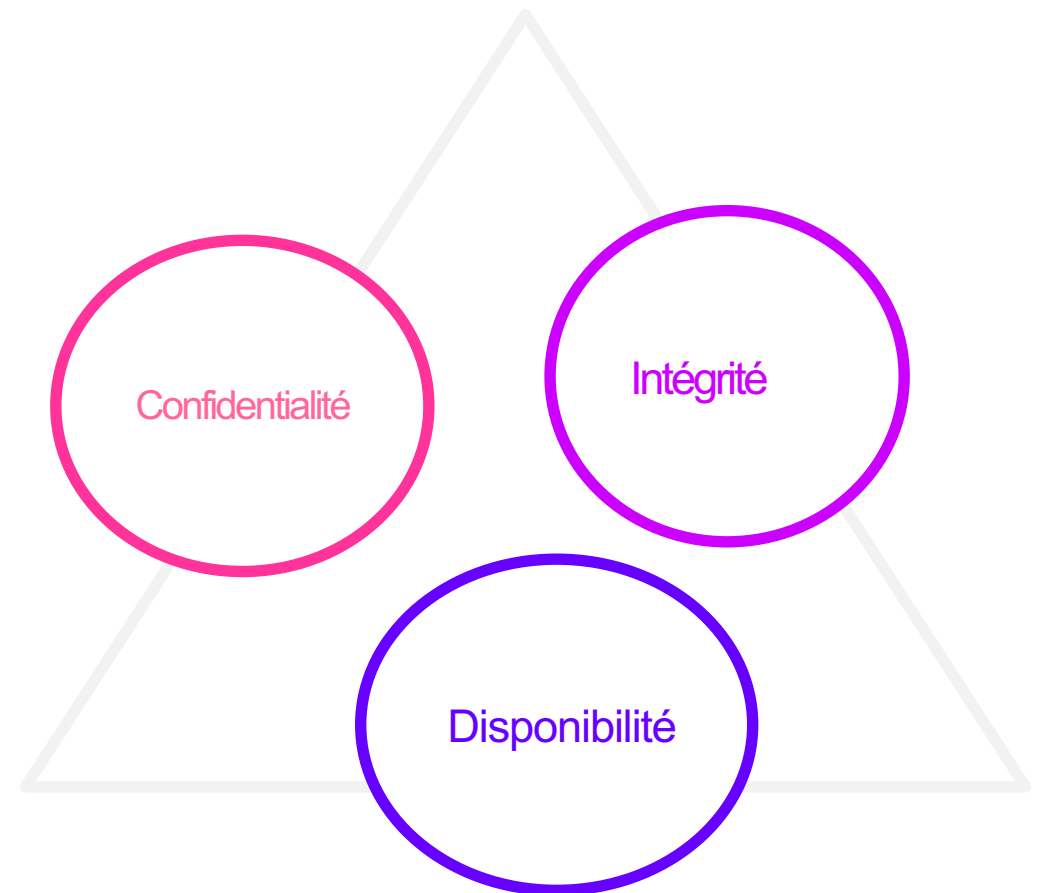
Vulnérabilités, menaces, attaques



Les Objectifs

Norme ISO/CEI27002

- Propriétés des actifs: le trio CID
- Identifie les objectifs de la sécurité de l'informatique selon 3 propriétés



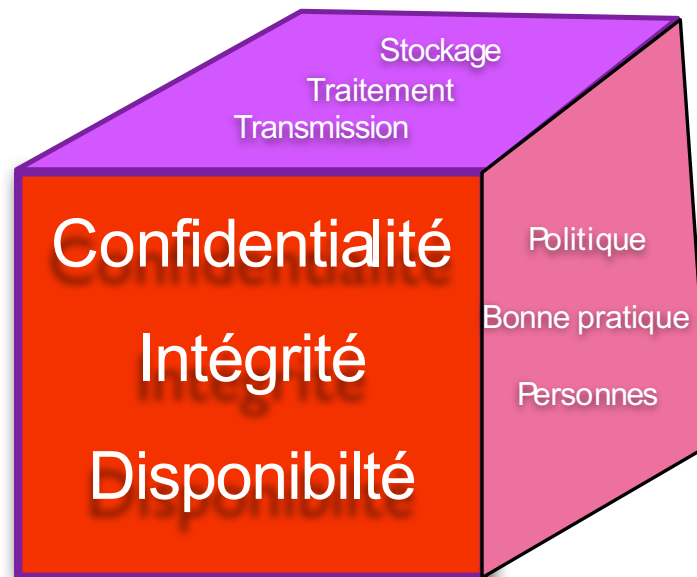
Les mesures

Services de sécurité

➡ Pour contrer les attaques, on doit définir des services de sécurité (objectifs de sécurité) à mettre en oeuvre

➡ Le trio CID constitue les principes fondateurs

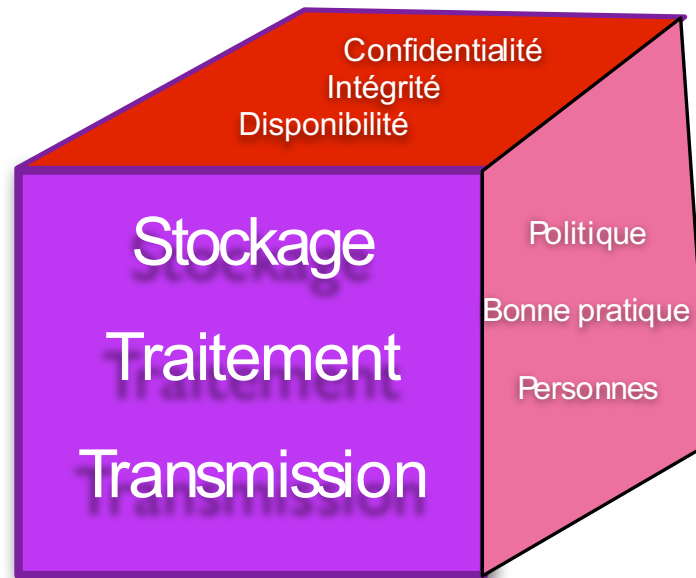
Cube de McCumber



Les mesures

Protection des données

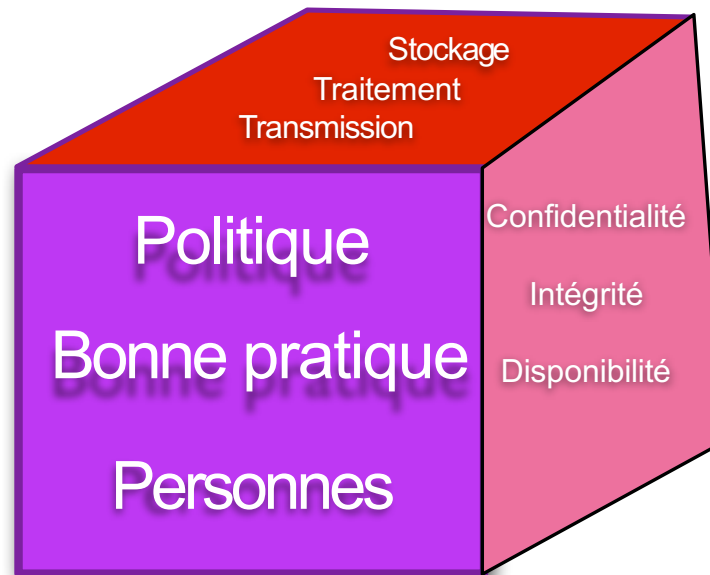
- Assurer la protection des données dans les trois états
- Le trio S2T constitue les principes fondateurs



Les mesures

Protection des données

- ❏ Les outils technologiques seuls ne suffisent pas pour mettre en échec les cybercriminels
- ❏ Il faut aussi développer des politiques de bonnes conduites et pratiques

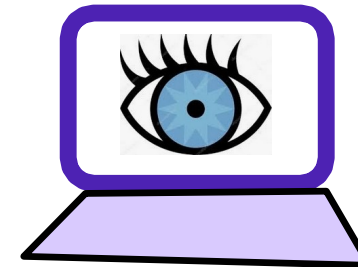


Les mesures menaces sur la confidentialité

☞ Surveillance du réseau (noms d'utilisateurs, les mots de passe et les numéros de carte bancaire, sont susceptibles d'être dérobées)

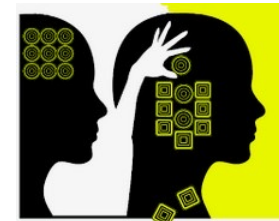


☞ Vol de fichiers de données et de fichiers de mots de passe



☞ Espionnage

☞ Ingénierie sociale

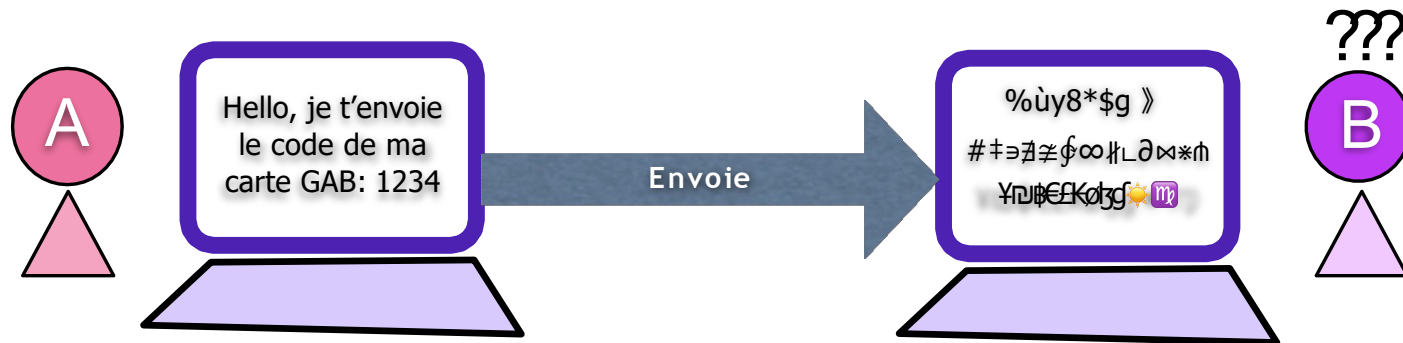


Les mesures

Contre-mesures pour la confidentialité

✓ Confidentialité des données

- par le **chiffrement** des données lors de leur transmission ou leur stockage
- Le **chiffrement** consiste à coder les données de sorte qu'elles soient illisibles.



Les mesures

Contre-mesures pour la confidentialité

✓ Le contrôle d'accès

- par l'authentification pour vérifier l'identité de l'utilisateur afin d'empêcher tout accès non autorisé

- par l'autorisation afin de définir les ressources auxquelles l'utilisateur a accès et les opérations qu'il peut effectuer (exemple les ACL, les droit RWX sur les fichiers etc.)



L'utilisateur A s'authentifie

A demande un accès au fichier0

	Propriétaire	Groupe	Tous
Fichier0	RWX	RW -	R - -
Fichier1	RWX	RW -	R - -

Les mesures

Contre-mesures pour la confidentialité

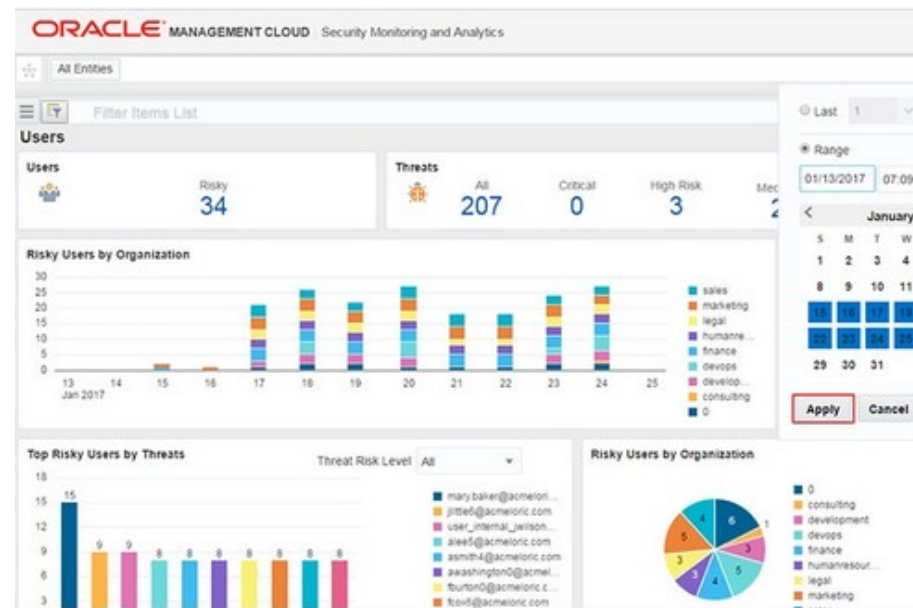
La **journalisation** par la suivi des actions des utilisateurs en fonction du temps.

Qui

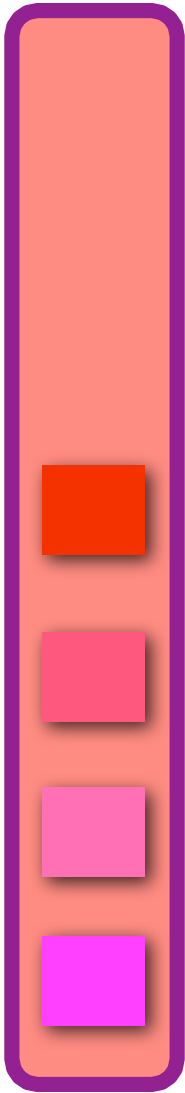
Quoi

Quand

Où



Les mesures menaces sur l'intégrité



☞ Modification ou suppression du trafic

☞ Virus, bombes logiques

☞ Erreurs humaines


☞ Portes dérobées


☞ Etc..




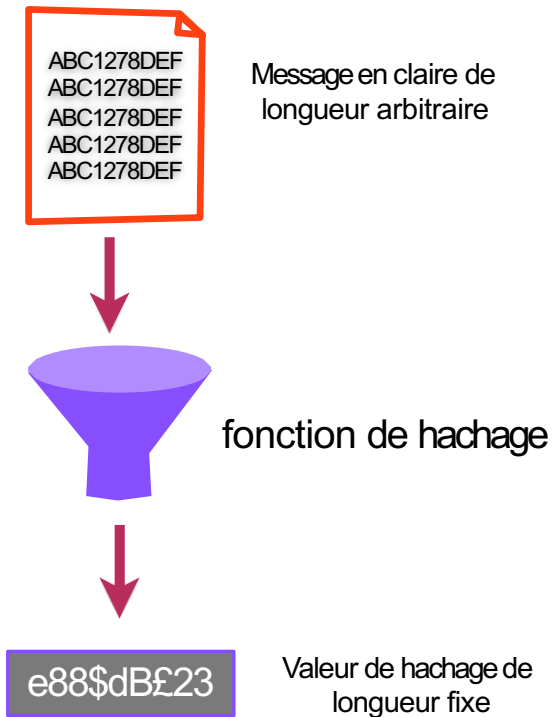
Les mesures

Contre-mesures sur l'intégrité

 **Le hachage**: garantie que les données ne subiront aucune modification, qu'elles soient au repos ou en transit.

 Il prend les données binaires (le message) et génère une représentation de longueur fixe, appelée valeur de hash ou condensé de message ou empreinte.

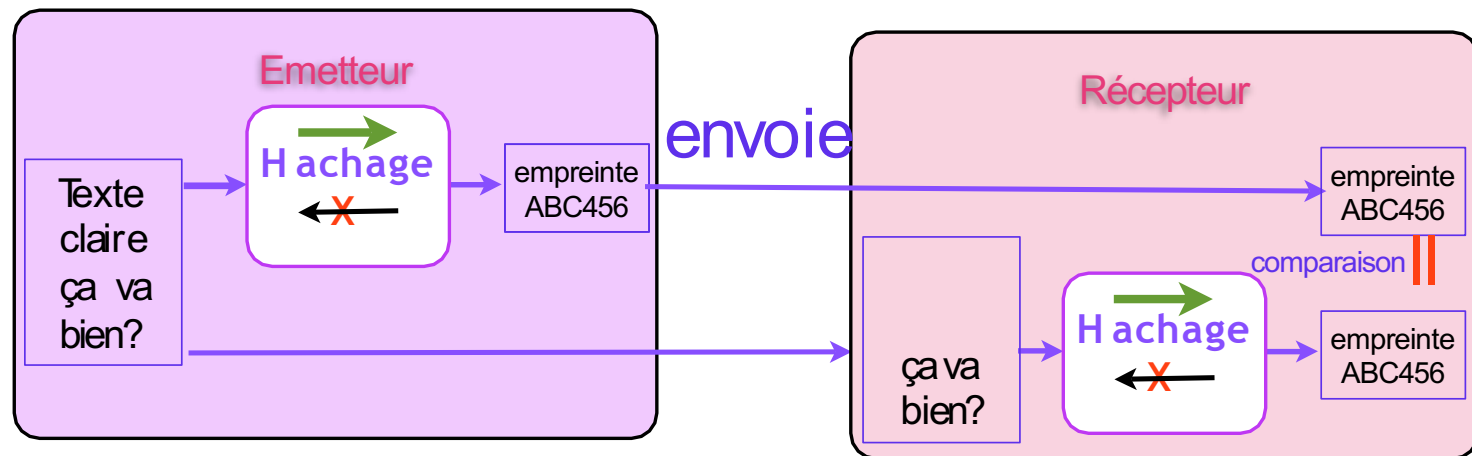
 Il s'agit de fonctions mathématique unidirectionnelle relativement simple à calculer, mais extrêmement difficile à inverser: MD5, SHA-1, SHA-256, SHA-512 etc....



Les mesures

Contre-mesures sur l'intégrité

Le hachage: envoie/réception

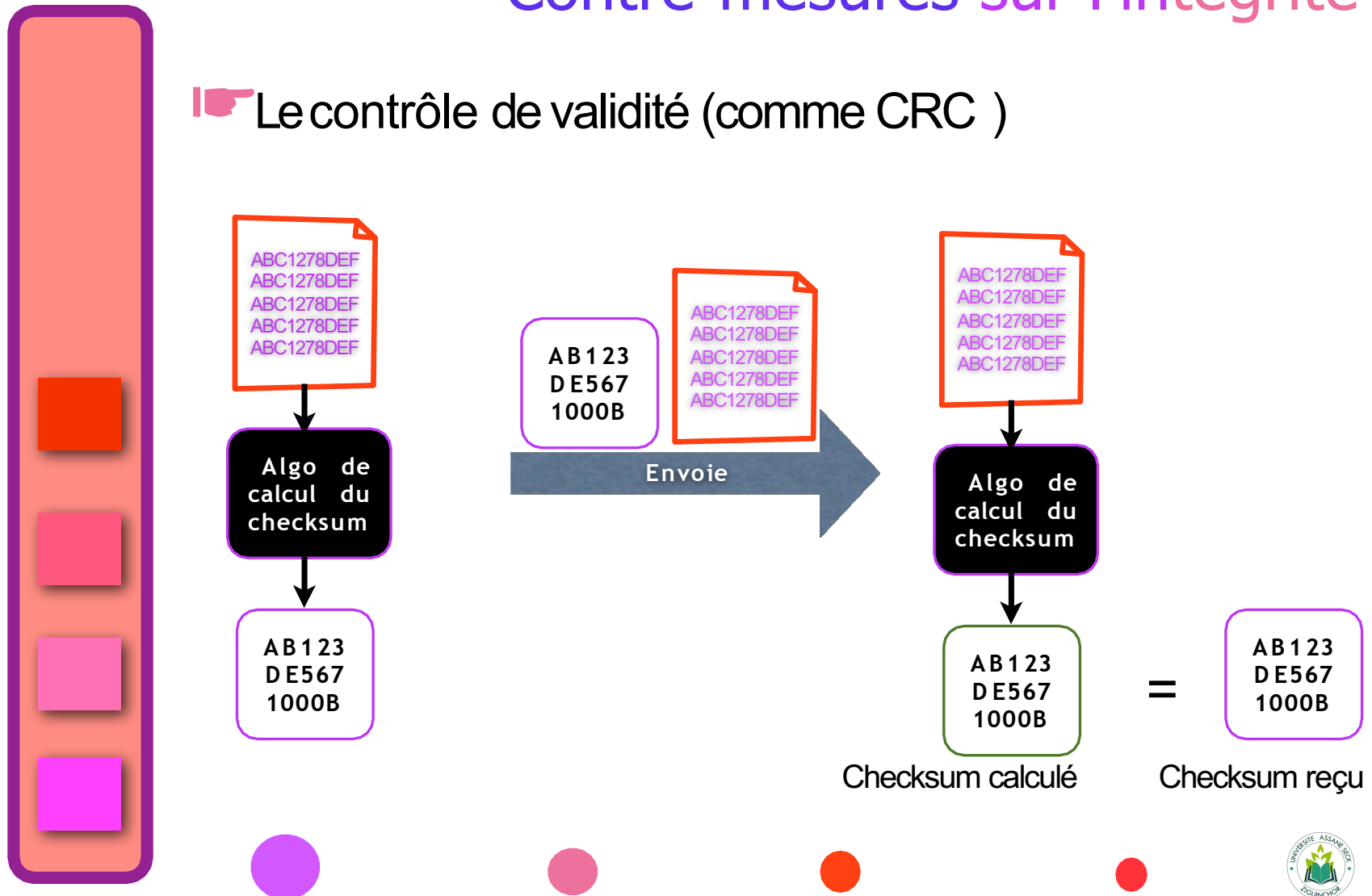


- empreinte identique= message accepté
- empreintes différentes= message rejeté

Les mesures

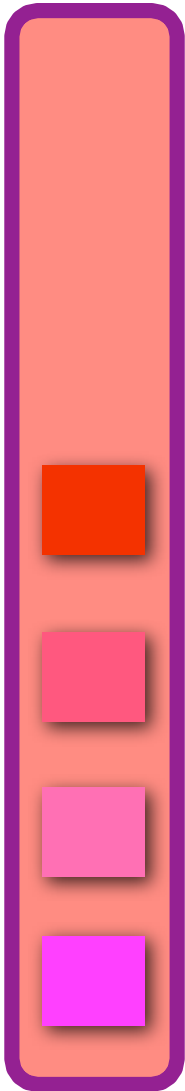
Contre-mesures sur l'intégrité

👉 Le contrôle de validité (comme CRC)



Les mesures menaces sur la disponibilité

- ❏ Déni de service (DoS, DDoS)
- ❏ Panne environnementale: une coupure de courant par exemple peut rendre le système inaccessible
- ❏ Panne matérielle: un serveur est endommagé et entraîne une perte de données confidentielles
- ❏ Panne logicielle: une application critique cesse de fonctionner
- ❏ Etc....



Les mesures

Contre-mesures sur la disponibilité

- ▮ La tolérance aux pannes
- ▮ Maintenance des équipements
- ▮ Mise à jour du système d'exploitation et des logiciels
- ▮ Sauvegarde
- ▮ Surveillance des activités inhabituelles
- ▮ Planification des sinistres

☒ Le concept des « cinq neuf » constitue l'une des pratiques de haute disponibilité les plus courantes. Ces cinq neuf correspondent à 99,999 %, soit un temps d'interruption inférieur à 5,26 minutes par an.

Sécurité Informatique

Approche traditionnelle

