




Les bases de la SSI

(Sécurité des Systèmes d'Information)

Alain Corpel

Enseignant-Chercheur en SSI
alain.corpel@utt.fr

Plan

- 
- Introduction
 - Quelques définitions
 - Pourquoi sécuriser un SI ?
 - Le DICP
 - La gestion des risques
 - Les 11 domaines
 - Quelques réflexions
 - Conclusion

Introduction



- Les Nouvelles Technologies de l'Information et de la Communication (NTIC) ont fortement impacté les organisations publiques et privées mais également notre vie quotidienne.
- Ses impacts sur les Systèmes d'Information ont permis d'augmenter considérablement la productivité des entreprises et ont facilité les différents échanges d'informations avec les individus.
- Elles ont donc été un formidable moteur de croissance de notre économie et sont devenues indispensables à la bonne marche de celle-ci.
- Malheureusement, l'ouverture de plus en plus importante des Systèmes d'Information et leurs interdépendances font qu'ils sont devenus l'un des maillons faibles et donc une cible facile pour qui voudrait nuire à une organisation.
- C'est pourquoi la Sécurité est devenu un enjeu majeur dans la mise en place et la gestion des Systèmes d'Information.

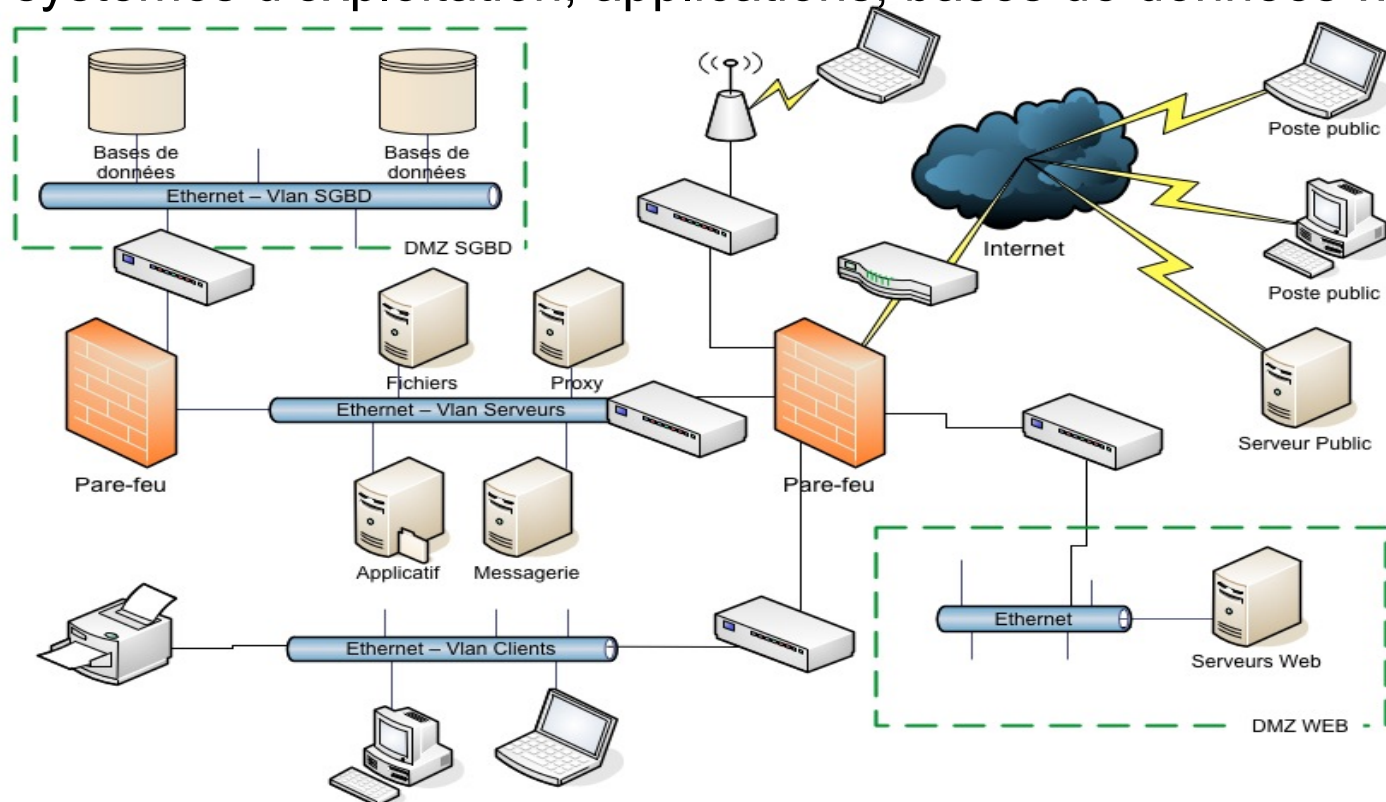


Quelques définitions



Système informatique

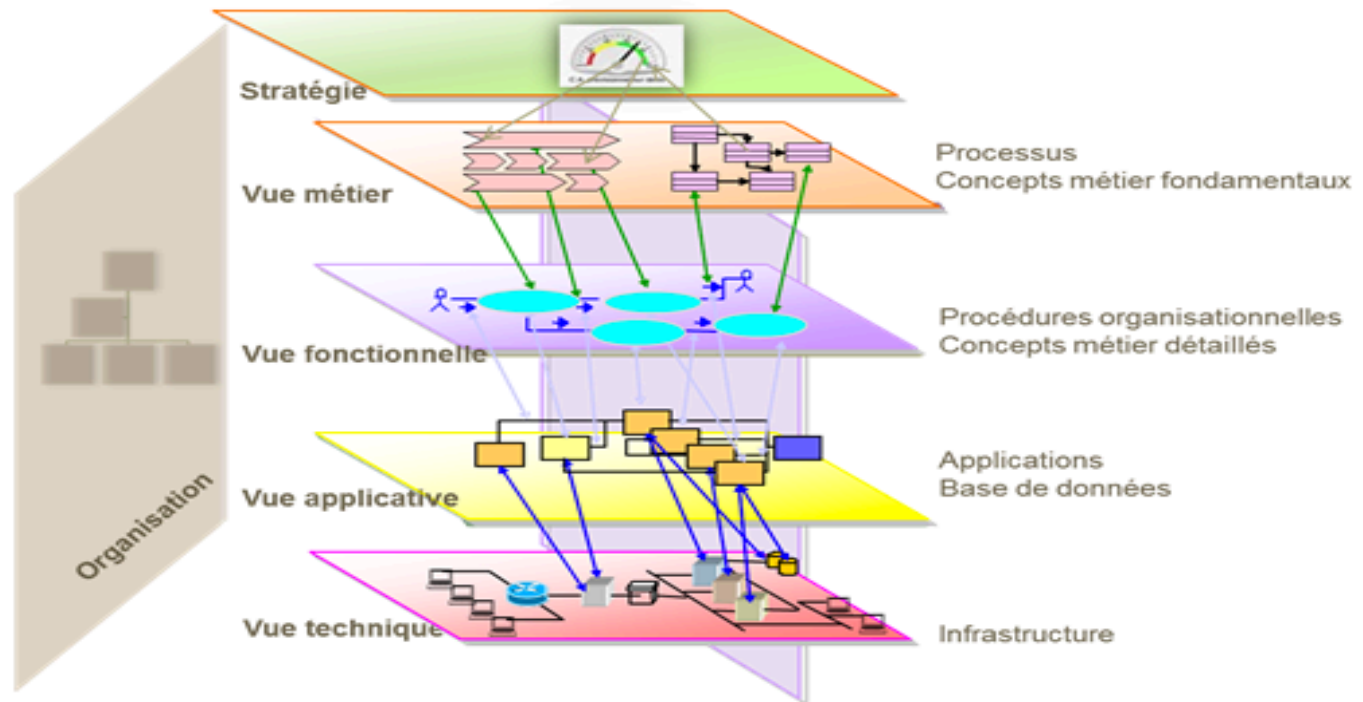
■ Un **système informatique** est un ensemble de dispositifs (matériels et logiciels) associés, sur lesquels repose un système d'information. Il est constitué généralement des serveurs, routeurs, pare-feu, commutateurs, imprimantes, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données ...





Système d'information

■ Un **système d'information** est un ensemble de moyens (humains, matériels, logiciels, etc.) organisés permettant d'élaborer, de traiter, de stocker et/ou de diffuser de l'information grâce aux processus ou services. Il intègre des sites, des locaux, des acteurs (partenaires, clients, employés, etc.), des équipements, des processus, des services, des applications et des bases de données...





Sécurité des Systèmes d'Information

■ La **sécurité d'un système d'information** est un ensemble de moyens **techniques**, **organisationnels**, **juridiques** et **humains** nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité notamment en terme de disponibilité, d'intégrité et de confidentialité (DIC).





Pourquoi sécuriser un SI ?

Les Enjeux



■ **Entreprises privées** : les organismes ou entreprises à but lucratif ont presque toujours la même finalité : c'est de réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son système d'information qui est l'un des moteur de développement mais également grâce à son savoir-faire. D'où la nécessité de garantir la sécurité du SI.

■ **Services publics** : les organismes publiques ont une finalité différente : rendre un service public à l'ensemble des personnes. Ceux-ci sont également très informatisés. La sécurité du SI notamment en terme de disponibilité est donc primordial.

■ **Opérateurs d'Importance Vitale (OIV)** : il s'agit des 12 secteurs d'activité (eau, santé, énergie, transport, télécoms et information, finances, alimentation, justice et forces de l'ordre, espace et recherche, industries stratégiques, armée et certains services publics) ayant des contraintes de sécurité fortes en terme de disponibilité intégrité et confidentialité.




Les Vulnérabilités

■ **Humaines** : l'être humain de par sa nature est vulnérable. C'est même le maillon faible dans le domaine de la SSI. La plupart des vulnérabilités humaines proviennent d'erreurs (négligence, manque de compétences, oublis, erreurs de saisie ...).

■ **Technologiques** : le tout informatique et le développement rapide des applications a eu pour effet de multiplier les vulnérabilités dans les logiciels. Elles ont pour origine des erreurs de conception, de développement, d'implémentation, de maintenance, de configuration...

■ **Organisationnelles** : elles sont essentiellement dues à l'absence des documents formalisés, des procédures (notamment d'alertes, d'escalade ...), de circuits de validation suffisamment détaillés pour faire face aux problèmes de sécurité.

Les Menaces



■ **Origines naturelles** : incendies, inondations, foudre, séismes, épidémies ...

■ **Origines humaines** : fuites d'informations, malveillance, espionnage, vol, modification, chantage, usurpation d'identités, grèves ...

■ **Origines juridiques** : nouvelles réglementations, changements administratifs, changements de politique locale ...

Les Attaques



■ **Définition** : elles représentent le fait d'exploiter une ou plusieurs vulnérabilités. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas forcément exploitables.

■ **Facteur aggravant** : les vulnérabilités exploitables à distance sont les plus dangereuses et facilitent donc grandement les attaques.

■ **Types d'attaques** : elles sont classées en 2 catégories

- **Les attaques passives** : consistent à écouter sans modifier les données ou le fonctionnement d'un SI

- **Les attaques actives** : consistent à modifier, voler ou détruire des données, perturber le bon fonctionnement d'un SI pouvant aller jusqu'au Dénial de Service (DOS et DDOS)

Synthèse



■ **Asset** : ressource

■ **Menace (en anglais « threat »)** : représente le type d'action (interne ou externe) susceptible de nuire aux ressources de l'entreprise

■ **Vulnérabilité (en anglais « vulnerability », appelée parfois faille ou brèche)** : représente le niveau d'exposition face à la menace dans un contexte particulier

■ **Contre-mesure ou parade** : c'est l'ensemble des actions mises en oeuvre en prévention de la menace

■ **Impact** : c'est la conséquence sur l'entreprise de la réalisation d'une menace

■ **Risque** : Combinaison d'une menace et des pertes qu'elle peut engendrer. C'est-à-dire de la potentialité de l'exploitation de vulnérabilité par un élément menaçant et de l'impact sur l'organisme

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité} \times \text{Potentialité}}{\text{Contre-mesure}}$$

Le Risque

■ **La Sécurité des Systèmes d'Information** : c'est une gestion de risques un peu comme pour les assurances.

■ **Comment gérer un risque** : il y a 4 manières de gérer le risque.

● **Ne rien faire** : l'impact est considéré moins coûteux que la mise en place d'une contre-mesure et/ou la probabilité de survenance de réalisation de la menace est très faible voire nulle

● **Suppression** : mise en place d'une contre-mesure pour contrer le risque

● **Réduction** : mise en place d'une contre-mesure pour réduire l'impact. Le risque résiduel est ainsi considéré comme acceptable

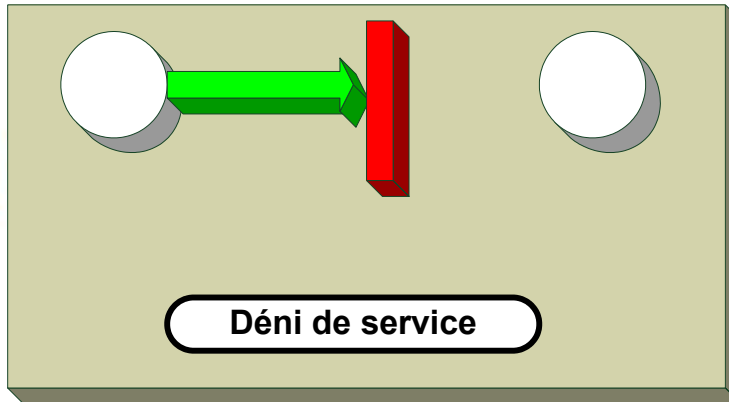
● **Transfert** : dans certains cas et pour certains risques, il est possible de les transférer vers un assurance (attaques, e-réputation ...)



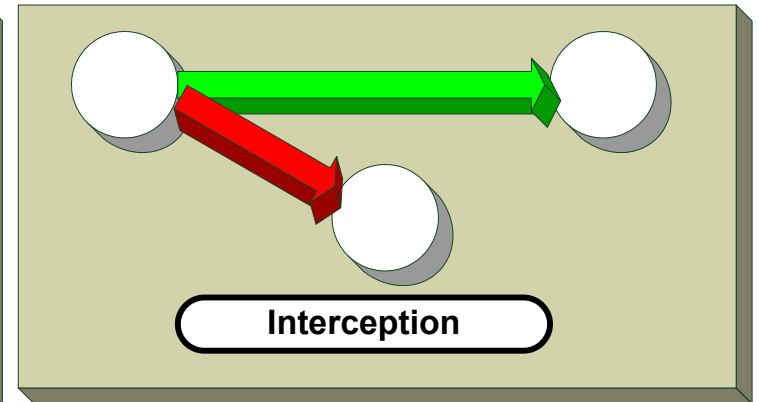
Le DICP



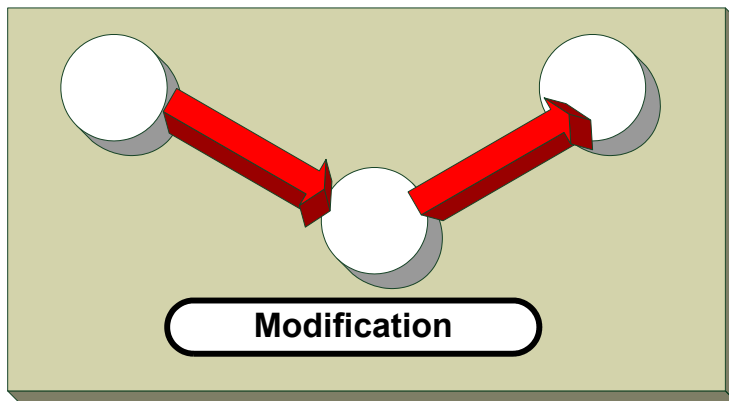
Menaces vs Risques



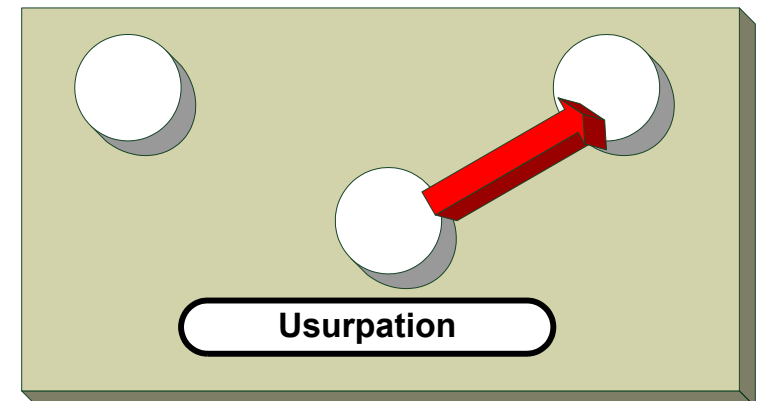
Menace sur la disponibilité



Menace la confidentialité



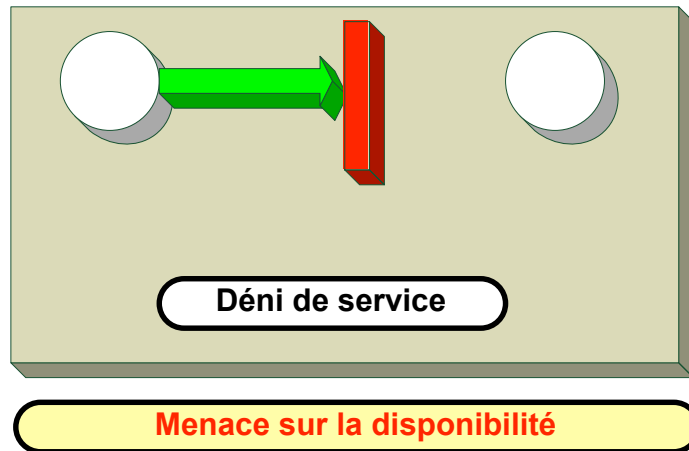
Menace l'intégrité



Menace l'authenticité



Disponibilité (Availability)

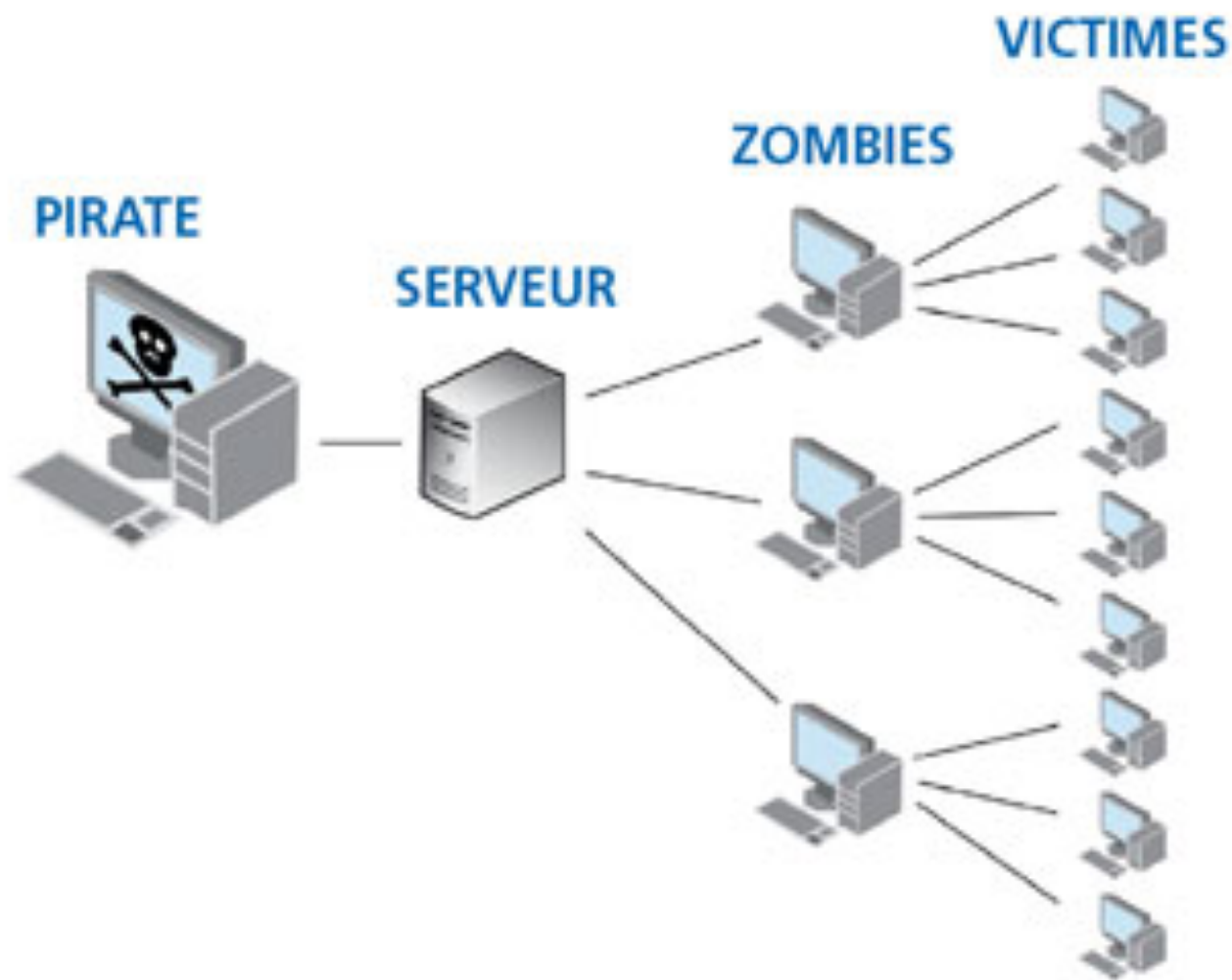


■ **Définition** : la disponibilité d'un système est une mesure de performance qu'on obtient en divisant la durée durant laquelle ledit système est opérationnel par la durée totale durant laquelle on aurait souhaité qu'il le soit. Elle se mesure en pourcentage (**exemple** : 99,99% correspond à une perte de disponibilité de 52 minutes et 33,6 secondes par an)

■ **Menaces** : les pannes font partie des principales menaces ainsi que le déni de service (DOS) et le déni de service distribué (DDOS)

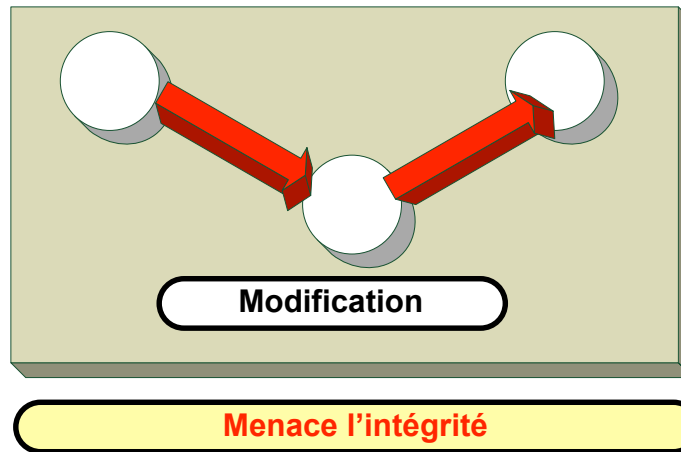


Déni de Service Distribué (DDOS)





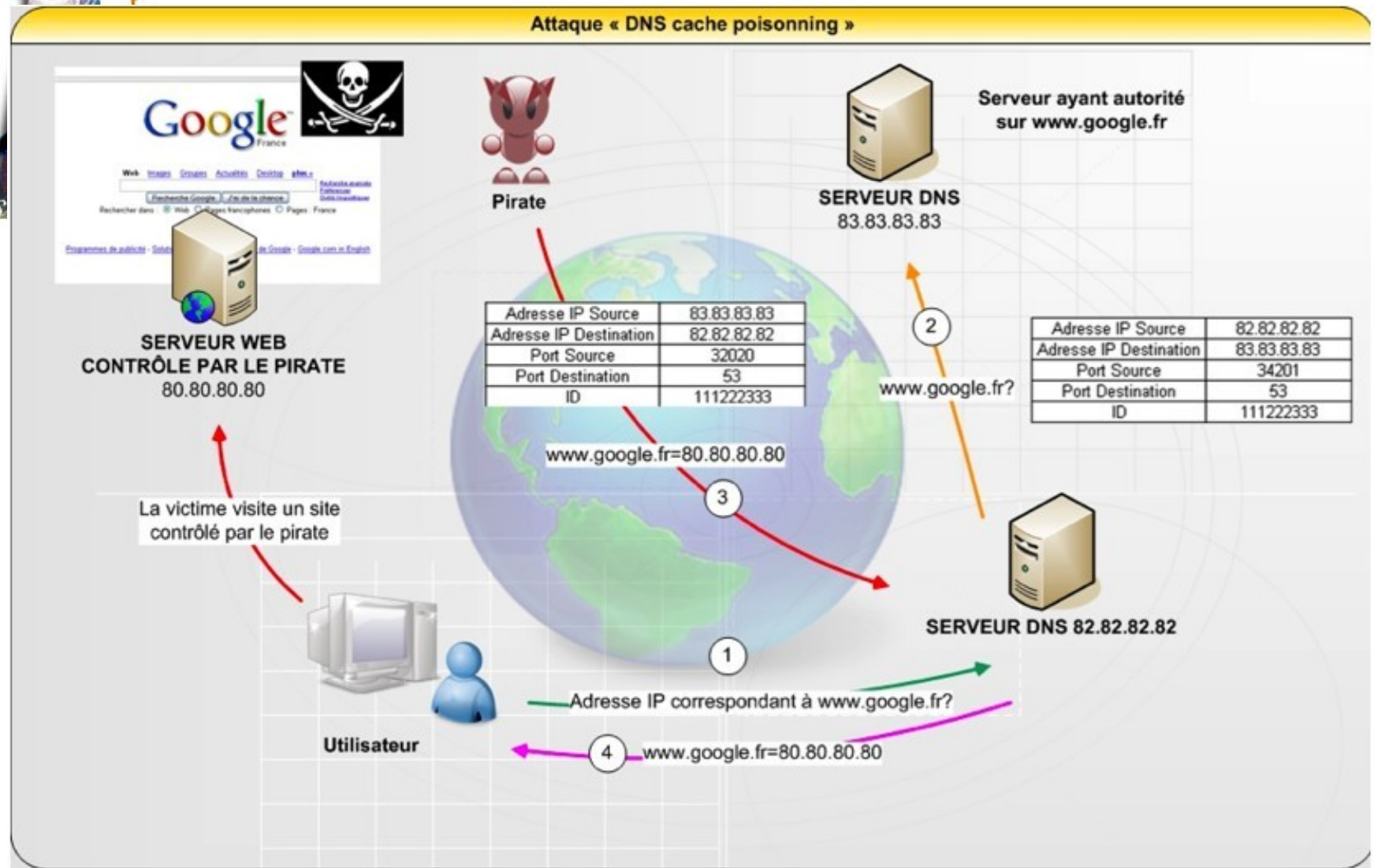
Intégrité (Integrity)



■ **Définition** : l'intégrité désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle.

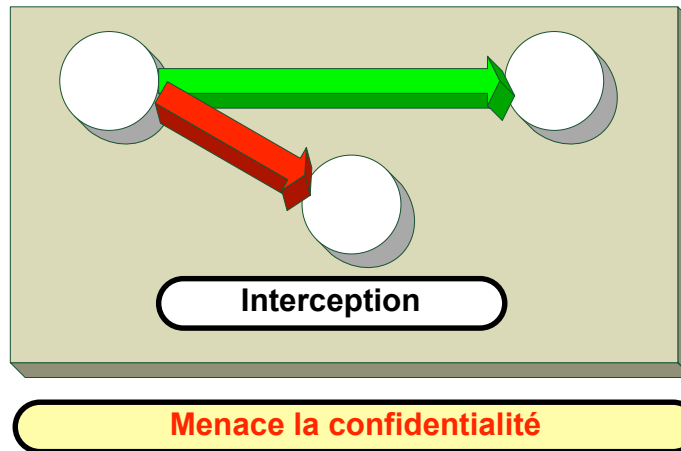
■ **Menaces** : les erreurs de saisie font partie des principales menaces ainsi que tout ce qui concerne les accès non autorisés aux données suite à des erreurs d'habilitation ou à des actes malveillants.

Empoisonnement des serveurs DNS





Confidentialité (Confidentiality)

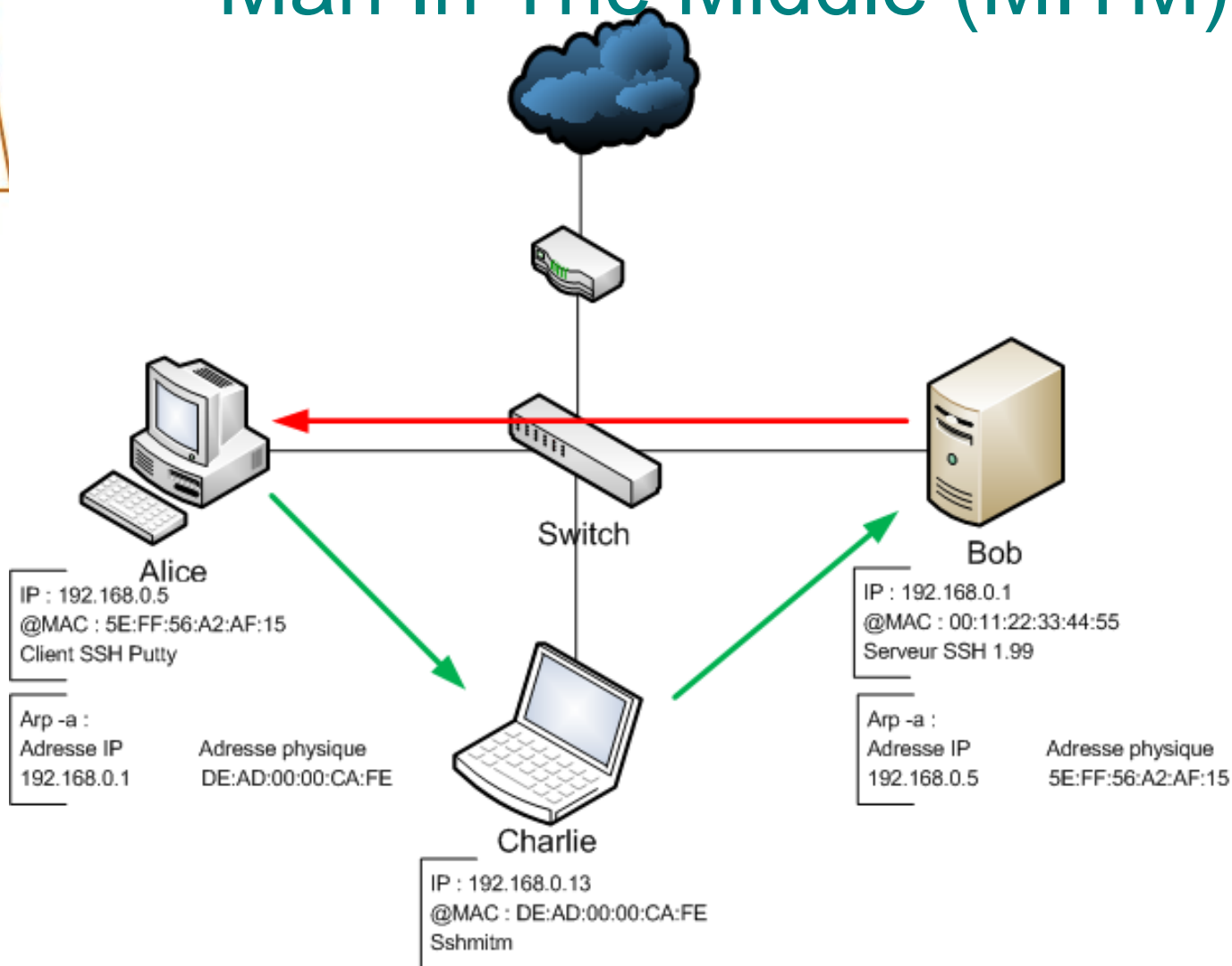


■ **Définition** : la confidentialité est le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé. Le principe de base est donc qu'une donnée ne doit être accessible que par les personnes qui ont des droits sur cette donnée. C'est le principe du moindre privilège.

Menaces : la négligence humaine (exemple : vol ou perte d'un smartphone ou d'un ordinateur portable) est l'une des principales menaces sur la confidentialité au même titre que l'interception des données.

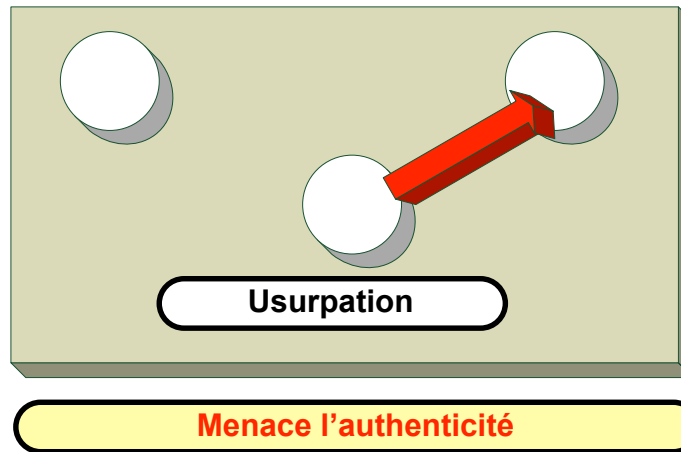


L'attaque de l'homme du milieu Man In The Middle (MITM)





Preuve (Evidence)

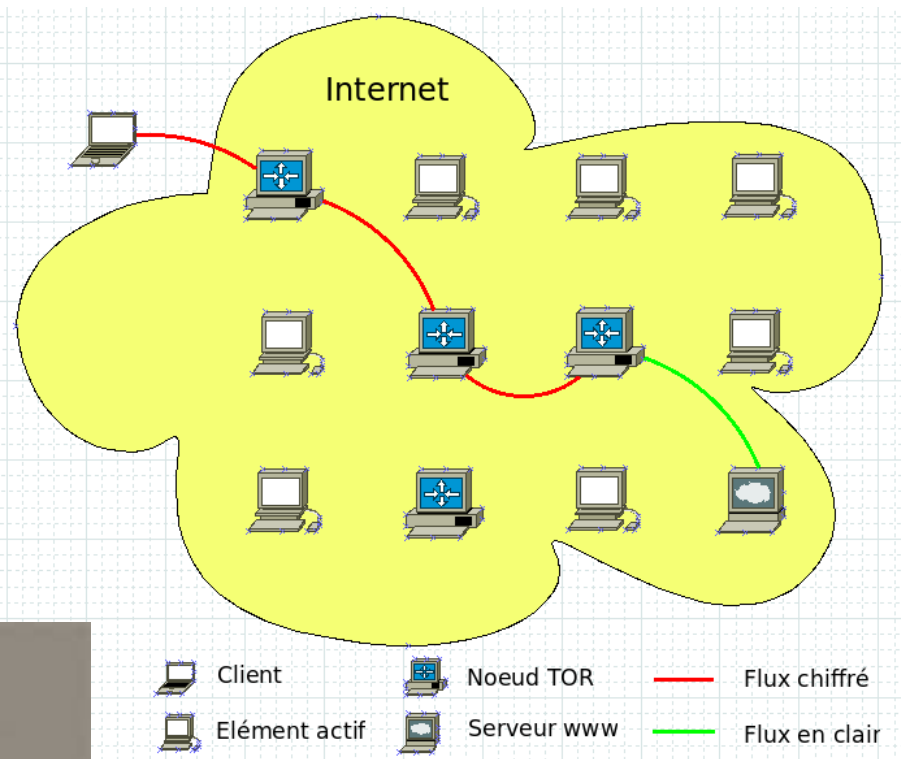


■ **Définition** : la preuve (ou imputabilité ou traçabilité) est le fait d'avoir la possibilité de remonter jusqu'à l'origine d'un événement et cela de manière sûre et fiable. Cela inclut également la non répudiation : un utilisateur ne peut nier avoir effectué une action ou reçu une information

■ **Menaces** : l'absence de journalisation est l'une des principales menaces ainsi que l'usurpation d'identité ou encore l'utilisation de réseaux et/ou de proxies (serveurs mandataires) permettant un certain anonymat.



Usurpation



Tor



Authentification

■ **Définition** : l'authentification est la procédure qui consiste, pour un système informatique, à **vérifier l'identité** d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...).

■ Pour s'authentifier → au moins 2 éléments


- Identifiant (exemple : login)
- Un ou plusieurs éléments d'authentification (exemples : password, OTP, certificat, biométrie, RFID+password ...)

■ 3 facteurs d'authentification :

- Ce que nous savons (mot de passe, code pin ...)
- Ce que nous avons (une carte à puce, un token, un I-key,...)
- Ce que nous sommes (empreinte, signature, reconnaissance vocale, ...)

■ **Authentification Forte** → utilisation d'au moins 2 facteurs parmi les 3.

Habilitation



■ **Définition** : l'habilitation consiste à vérifier si une entité (une personne, un ordinateur, ...) demandant d'accéder à une ressource a les droits nécessaires pour le faire. Une fois authentifiées les actions de l'entité doivent être encadrées.

■ L'habilitation offre ainsi la possibilité d'accéder à des ressources physiques (**exemple** : un bâtiment, un local, un pays) ou logiques (**exemple** : un système d'exploitation ou une application informatique spécifique).

■ L'habilitation comprend généralement 3 composantes :

- Un mécanisme **d'authentification** de l'entité
- Un mécanisme **d'autorisation** (l'entité peut être authentifiée mais ne pas avoir le droit d'accéder à cette ressource à ce moment)
- Un mécanisme de **traçabilité**



La gestion des risques



Comme une assurance (1/2)

■ La Sécurité des Systèmes d'Information peut être résumée à une gestion des risques au même titre qu'une assurance.

■ La démarche peut donc être définie de la manière suivante :

● **Evaluer les risques et leur criticité :**

- Quels risques et quelles menaces ?
- Sur quelles données et quelles activités ?
- Avec quelles conséquences ?

Cela débouche sur une « cartographie des risques ». De la qualité de cette cartographie dépend la qualité de la sécurité qui va être mise en œuvre.

● **Rechercher et sélectionner les parades :**

- Que va-t-on sécuriser, quand et comment ?

Etape difficile des choix de sécurité : dans un contexte de ressources limitées (en temps, en compétences et en argent), seules certaines solutions pourront être mises en œuvre.

Comme une assurance (2/2)



■ ...:

● **Mettre en œuvre les protections, et vérifier leur efficacité :**

C'est l'aboutissement de la phase d'analyse et c'est là que commence vraiment la sécurisation du système d'information. Une faiblesse fréquente de cette phase est d'omettre de vérifier que les protections sont bien efficaces (plan de secours et plan de reprise non testés, tests d'intrusions jamais effectués, sauvegardes non testées, utilisateurs non sensibilisés, gestion des mises aléatoires ...)

■ **Attention**, comme pour une assurance le retour sur investissement (ROI) n'est pas évident voire impossible à calculer.



L'outil de base

- Il existe de très nombreux outils permettant de mettre en œuvre une véritable démarche de sécurité.
- Le premier de ces outils est la méthode d'analyse de risques. Différentes méthodes existent :

- **MEHARI** (MEthode Harmonisée d'Analyse des Risques) : analyse des vulnérabilités et des risques. Elle permet d'avoir une vision globale et stratégique de la SSI

- **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité) : permet de définir les objectifs de sécurité pour répondre à des besoins déterminés. Elle permet d'appréhender le contexte de sécurité.

- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) : permet de faire une analyse de risques à l'aide d'un catalogue de bonnes pratiques

- **CRAMM** (Ccta Risk Analysis and Management Method) : elle permet de définir les ressources à sécurisées, de faire une analyse de risques et des vulnérabilités puis de définir et choisir les mesures de sécurité



Le résultat de la SSI



Le dispositif de
sécurité

La consigne

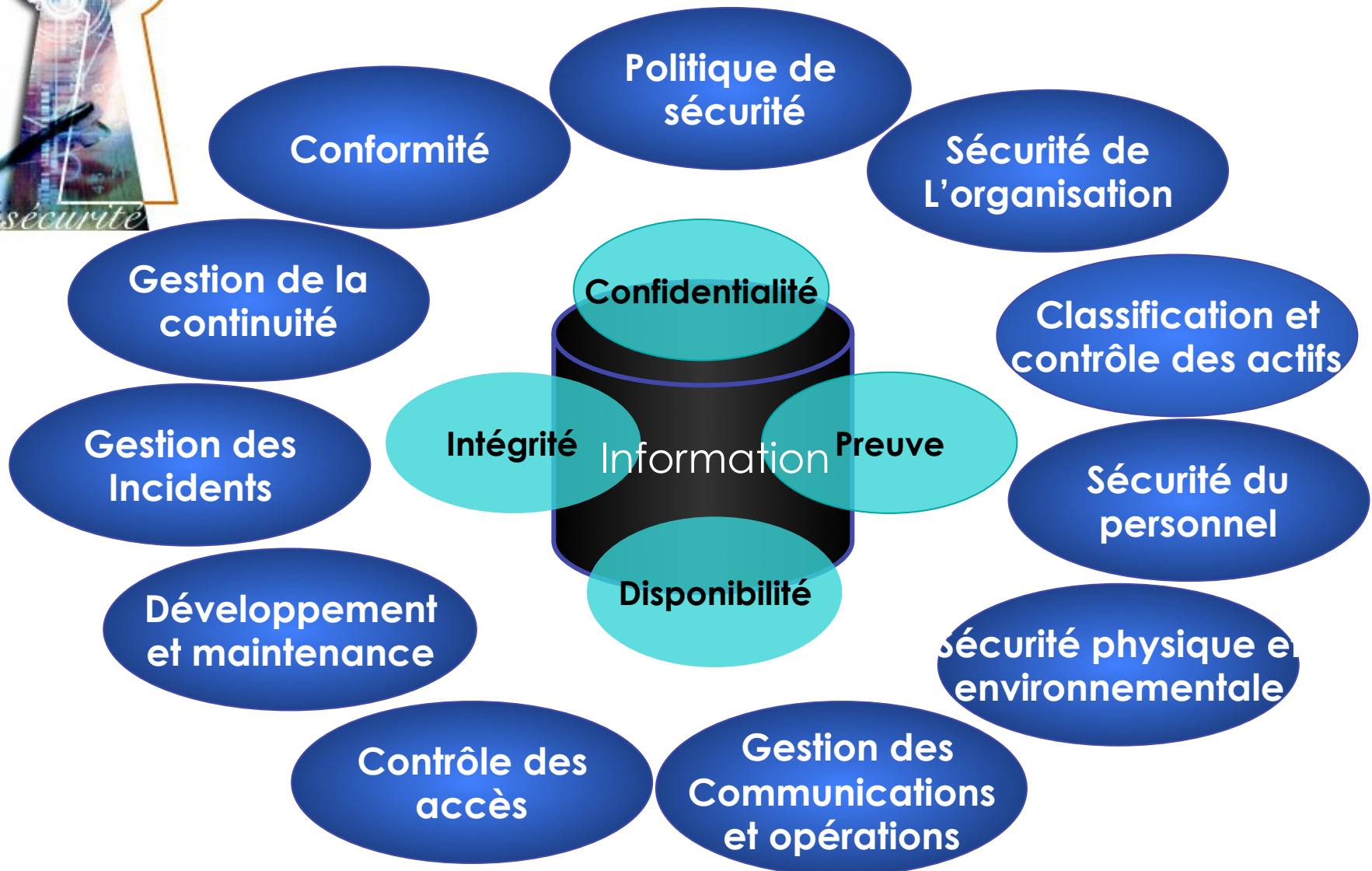
La méthode de
contournement



Les 11 domaines (selon l'ISO 27002 – Version 2005)



ISO 27002 (version 2005)





Politique de sécurité des systèmes d'information (1/11)

- La Politique de Sécurité des Systèmes d'Information (PSSI) est la première brique et la pierre angulaire de toute démarche en SSI.
- Elle doit au moins comporter les mesures suivantes :
 - Liste des points à aborder dans la PSSI
 - Mise à jour régulière de la PSSI

Organisation de la sécurité des systèmes d'information (2/11)



- La SSI n'est pas seulement un problème technique, c'est également un problème d'organisation.
- Elle doit au moins comporter les mesures suivantes :
 - Organisation interne
 - Relations avec les tiers

Gestion des biens (3/11)



- Chaque actif/ressource (Asset) de l'entreprise doit être inventoriée et un responsable par ressource doit être désigné.
- Elle doit au moins comporter les mesures suivantes :
 - Responsabilités relatives aux biens
 - Classification des informations



Sécurité liée aux ressources humaines (4/11)

- L'humain étant le maillon faible, il est indispensable d'en tenir compte dans une démarche SSI.
- Elle doit au moins comporter les mesures suivantes :
 - Avant l'embauche
 - Pendant la durée du contrat
 - Au départ du collaborateur
- Attention, **collaborateur** est à prendre au sens large :
 - Salarié en CDI, CDD ...
 - Stagiaires
 - Intérimaires
 - Personnel extérieur

Sécurité physique et environnementale (5/11)



- Souvent négligée, la sécurité physique doit faire l'objet d'une attention particulière.
- Elle doit au moins comporter les mesures suivantes :
 - Sécurité des locaux
 - Sécurité du matériel



Gestion de l'exploitation et des télécommunications (6/11)

- Probablement, le domaine le plus critique dans une démarche de sécurisation. Elle intègre aussi bien des aspects organisationnels que techniques.
- Elle doit au moins comporter les mesures suivantes :
 - Procédures d'exploitation et responsabilités
 - Prestation de service par un tiers
 - Planification et acceptation du système
 - Protection contre les codes malveillants
 - Sauvegarde
 - Gestion de la sécurité des réseaux
 - Manipulation des supports
 - Echange des informations
 - Commerce électronique
 - Surveillance



Contrôle d'accès (7/11)

- Ce domaine concerne les contrôles d'accès logiques. Ceux concernant l'accès aux locaux ont été traités dans le domaine « Sécurité physique et environnementale ».
- Elle doit au moins comporter les mesures suivantes :
 - Politique
 - Utilisateurs
 - Responsabilités des utilisateurs
 - Réseau
 - Système d'exploitation
 - Applications
 - Informatique mobile et télétravail



Acquisition, développement et maintenance des systèmes d'information (8/11)

- Le développement (à fortiori la maintenance) est souvent le « parent pauvre » de la SSI notamment parce qu'elle concerne les informaticiens : population la plus à risque et la plus difficile à gérer.
- Elle doit au moins comporter les mesures suivantes :
 - Exigences de sécurité
 - Bon fonctionnement des applications
 - Chiffrement
 - Systèmes de fichiers
 - Développement et support
 - Vulnérabilités



Gestion des incidents liés à la sécurité de l'information (9/11)

- Domaine apparu récemment dans la SSI, il n'en est pas moins aussi important que les 10 autres domaines.
- Elle doit au moins comporter les mesures suivantes :
 - Signalement des incidents
 - Gestion des incidents



Gestion du plan de continuité de l'activité (10/11)

- Les plans de reprise d'activité (PRA) et de continuité d'activité (PCA) sont indispensables pour la survie d'une entreprise dans le cas où elle subirait un sinistre majeur
- Elle doit au moins comporter les mesures suivantes :
 - Appréciation des risques
 - Elaboration et mise en œuvre des plans
 - Tests
 - Mise à jour des plans

Conformité (11/11)

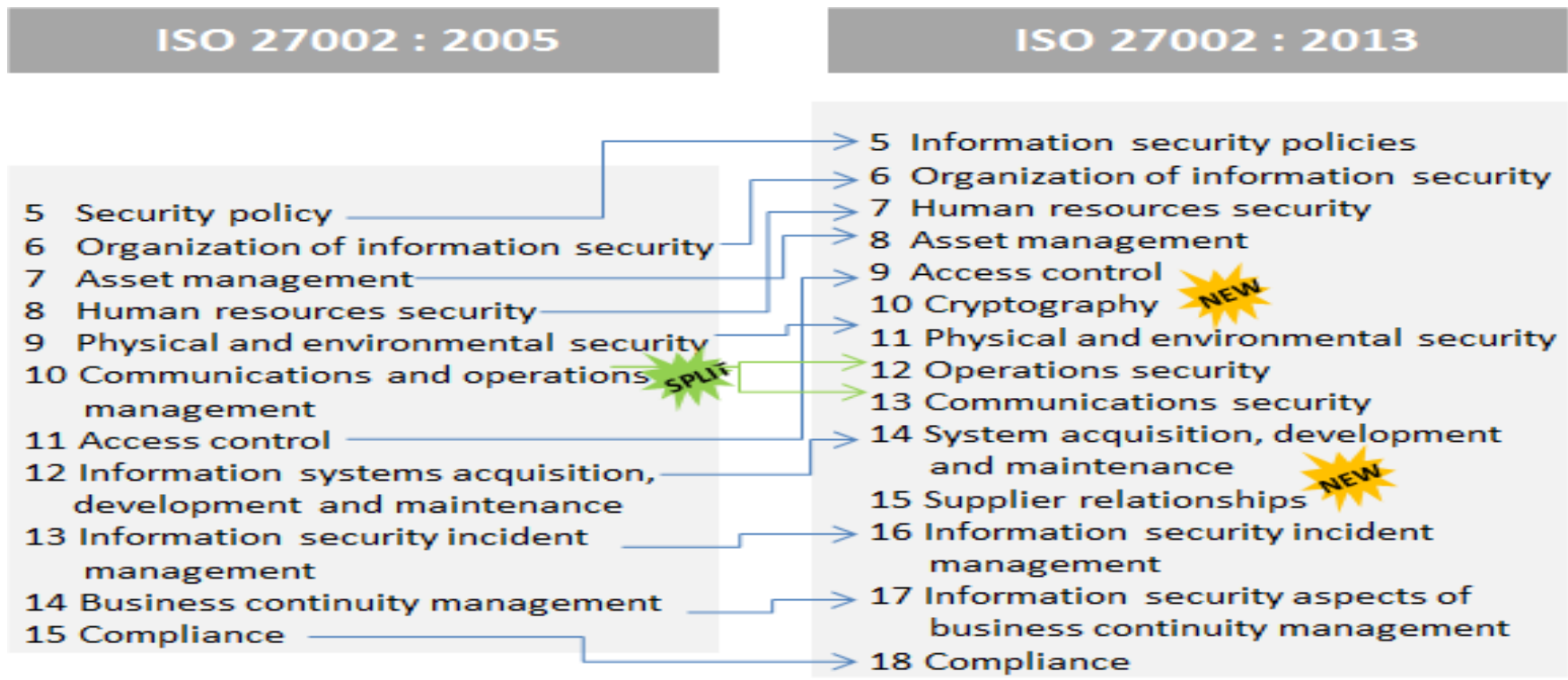


- Le dernier domaine n'est pas à négliger même s'il semble à la périphérie de la SSI, les problèmes juridiques et normatifs prenant de plus en plus d'importance dans nos sociétés.
- Elle doit au moins comporter les mesures suivantes :
 - Réglementation
 - Procédures internes
 - Audits du SI



ISO 27002 : ver. 2005 VS ver. 2013 (1/2)

ISO 27002:2005	ISO 27002:2013
11 chapitres	14 chapitres
38 objectifs de sécurité	35 objectifs de sécurité
133 Mesures de sécurité	114 Mesures de sécurité





ISO 27002 : ver. 2005 VS ver. 2013 (2/2)

- Politique de sécurité → Politiques de sécurité de l'information
- Gestion de l'exploitation et des télécommunications scindée en 3 parties :
 - Sécurité liée à l'exploitation (chap. 12 - ver. 2013)
 - Sécurité des télécommunications (chap. 13 - ver. 2013)
 - Relation avec les fournisseurs (chap. 15 - ver. 2013)
- Acquisition, développement et maintenance des systèmes d'information scindée en 2 parties :
 - Cryptographie (chap. 10 - ver. 2013)
 - Acquisition, développement et maintenance des systèmes d'information (chap. 14 - ver. 2013)
- Gestion du plan de continuité de l'activité → Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité (chap. 17 - ver. 2013)



Quelques réflexions

Soyons pragmatique ...

■ **Single point of failure** : le moindre grain de sable peut faire tomber les meilleures solutions techniques et organisationnelles déployées.

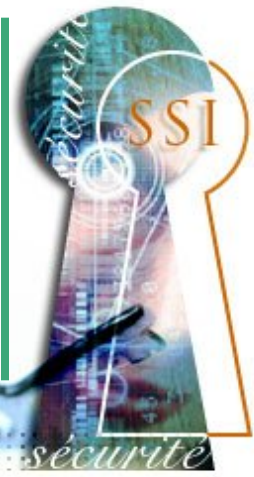
■ **Ne pas être plus royaliste que le roi** : trop de sécurité (contraintes) tue la sécurité, il faut trouver le juste milieu.

■ **Sécurité (security) vs Sûreté (safety)** : sécurité = sûreté + malveillance.

■ **Restons humble** : le monde de la sécurité est très égocentrique et médiatisé notamment au cinéma et dans les séries.

■ **Sécurité à 100%** : cela n'existe pas.

■ **La risque vient de l'intérieur** : non seulement le sentiment de sécurité est fort donc la vigilance est moindre mais les mesures sont plus faibles que sur la périmétrie du SI.





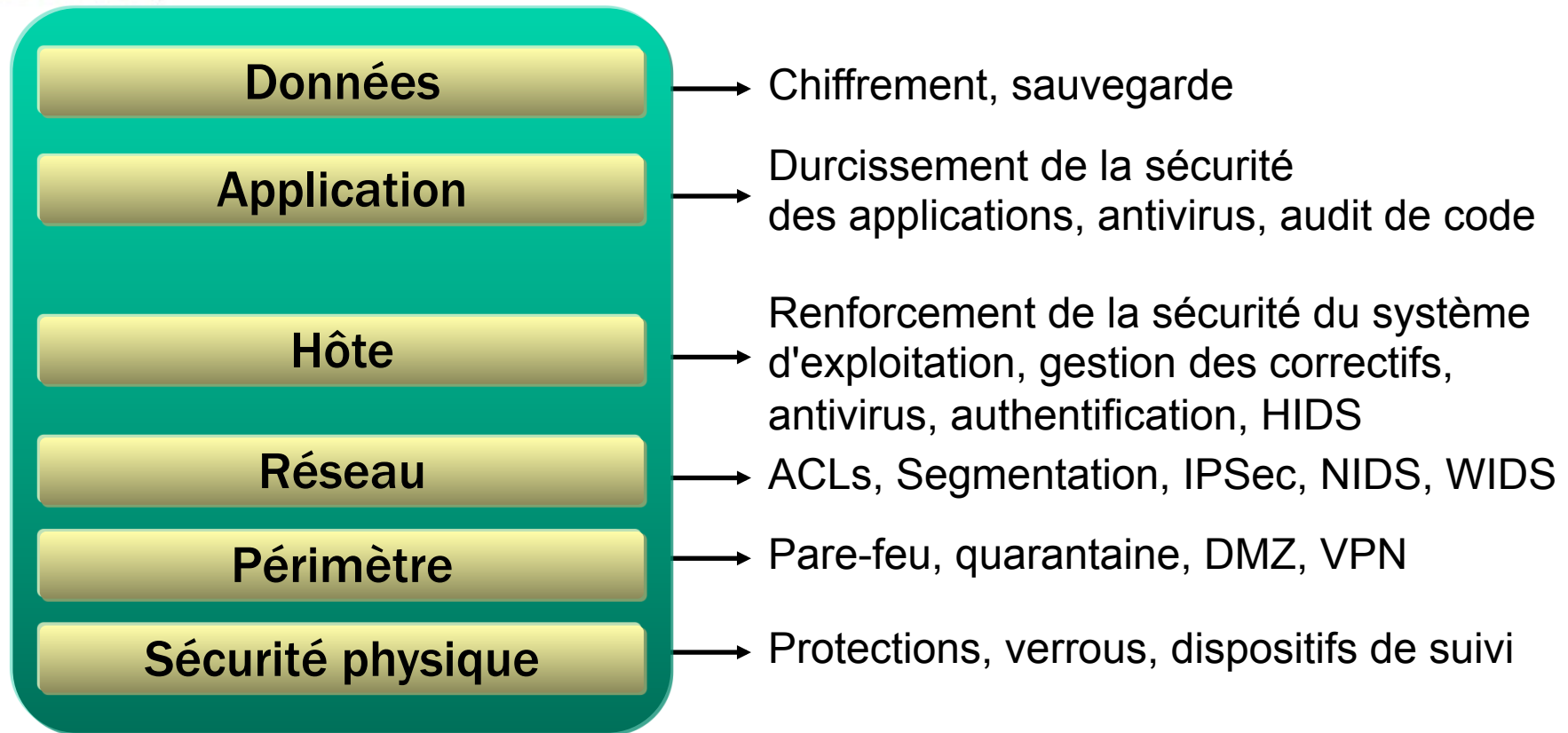
Les fausses bonnes idées

- **Tout autorisé sauf** : l'exhaustivité en termes de risques et de types d'attaques n'existent pas.
- **L'utilisateur n'y connaît rien** : ne jamais sous-estimé la créativité de l'utilisateur pour contourner une mesure de sécurité.
- **L'utilisateur sensibilisé nous protège** : la cupidité et certains centres intérêts diminuent la vigilance des utilisateurs.
- **Adopter les nouvelles technologies dès qu'elles sortent** : il faut toujours attendre un certain temps pour que la technologie soit stabilisée et donc sécurisée.
- **Nous ne sommes pas une cible** : toute organisation ou individu est une cible potentielle.
- **Les pirates sont des gens sympas** : la plupart du temps, il s'agit de criminels, les autres sont des individus utilisant des outils qu'ils ne maîtrisent pas.



La défense en profondeur

- Utilisation d'une approche en couches → réduit les chances de succès et augment la probabilité de détection d'un intrus.
- Chaque couche de sécurité doit être indépendante de la précédente.





Les 10 types de compétences

- **Réseaux** : protocoles, routeurs, commutateurs, plans d'adressage, services de base, Vlan, Vpn, Snmp...
- **Systèmes** : Windows, Unix/Linux.
- **Sécurité réseaux** : pare-feux, IDS/IPS, scanners, outils d'audits de vulnérabilités, monitoring, corrélation de logs, SIEM, Dmz...
- **Sécurité des systèmes** : antivirus, pare-feux applicatifs, "anti-tout », gestion des patches ...
- **Cryptographie** : symétrique, asymétrique, fonctions de hachage, signature, PKI, protocoles SSL/TLS.
- **Sécurité Internet** : messagerie, serveurs web, Dns, applications.
- **Mobilité et Nomadisme** : accès distants, sécurisation des réseaux sans-fil, gestion des périphériques, smartphones.
- **Programmation** : notions de programmation sécurisée (Assembleur, C, Java, Perl, Python, Shell, PHP, XML...).
- **Plan de secours et de reprise** : bonnes pratiques.
- **Méthodologies d'Audit** : Ebios, Méhari, critères communs, ISO 27001, 27002 et 27005 ...

Conclusion



■ Après avoir fait un rapide tour d'horizon de ce qu'est la Sécurité des Systèmes d'Information, nous voyons que le périmètre de celle-ci est relativement large allant des mesures techniques jusqu'aux mesures organisationnelles.

■ Il est important d'avoir une vision globale de la SSI incluant l'ensemble des domaines car elle a un rôle transversale vis à vis du Système d'Information. De même, il faut toujours avoir une démarche pro-active et non réactive.

■ Attention cependant, il faut rester vigilant et être prêt à réagir à une attaque réussie ou à un incident de sécurité. La mise en place de contre-mesures doit pouvoir être rapide car l'impact financier sur l'entreprise peut être important voire engager la survie de celle-ci.

■ Dernier point, la sécurité étant l'affaire de tous, il est primordial de sensibiliser l'ensemble des acteurs notamment les populations à risque que sont les VIPs et les informaticiens.