M1
Sécurité des systèmes d'informations
2023-2024

UNIVERSITE PARIS 8 VINCENNES-SAINT-DENIS
Christophe Villeneuve
@hellosct1
@hellosct1@mamot.fr

Session 5 : Gestion de la cybersécurité au sein d’une organisation

- Correction TP 4
- La sécurité au sein d’une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité
- Conseiller d’orientation
- L’organisation de sécurité moderne
- TP : Brainstorming
- Guide de conformité

- La sécurité au sein d’une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité
- TP : Brainstorming

Correction TP 4

- Sujet :
  - Identifier les piliers techniques et non techniques de la sécurité de réseau ?
- Réponse attendue :

  → Slides qui suivent
- Solution au sujet

  → Session 4 – Partie 1 : Sécurisation d’un réseau

Piliers techniques de la sécurité de réseau

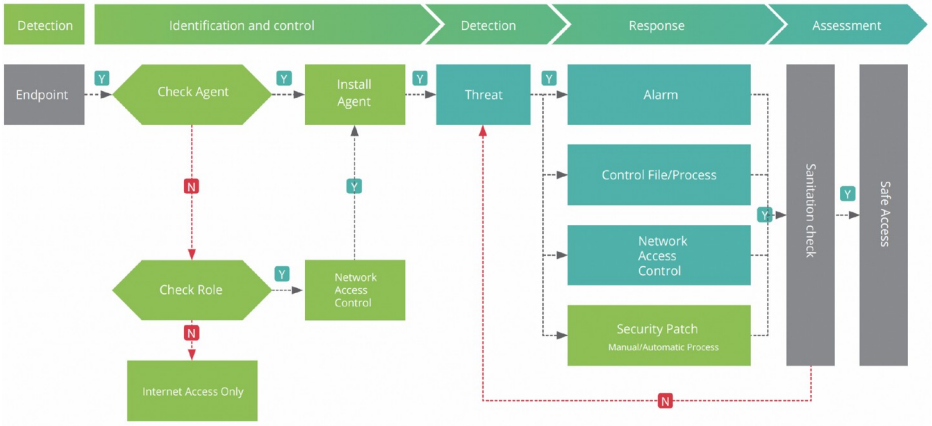
CORRECTION

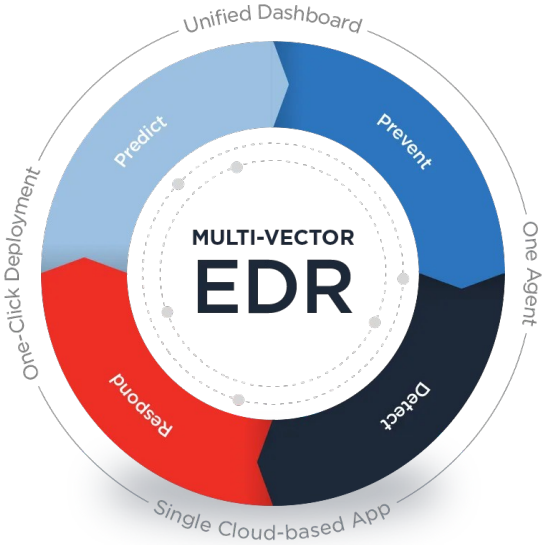
- 1 – Sécurité périmétrique
  - Les frontières sont devenues plus floues
    - La sécurité périmétrique reste toujours le premier rempart à mettre en place.
  - Indispensable
  - Protéger la frontière externe de l’entreprise des menaces extérieures pour éviter ou limiter les infections
    - malwares, cheval de Troie, etc
  - Actions :
    - Bien paramétrer ses firewalls
    - Etre très sélectif et granulaire dans les autorisations de flux

Piliers techniques de la sécurité de réseau

CORRECTION

- 2 – La sécurité Endpoint
  - Combattre l'infection une fois détectée grâce à des antivirus ciblés.
  - Maintenant
    - Les nouveaux malwares sont capable de « muter » afin d'éviter d'être détecté.
    - Virus « intraçables », qui utilisent les failles encore inconnues.
      - Solution :
        - type Endpoint Detection and Response (EDR).





Piliers techniques de la sécurité de réseau

CORRECTION

- 3 – La détection de menaces sur le réseau
  - Consiste à détecter
    - Les comportements non conventionnels
    - Retrouver les traces d'un attaquant sur le réseau de l'entreprise
      - logs, données, IA, etc.
  - Identifier les informations suspectes
    - dans un lot gigantesque de données grâce à l'automatisation
      - Décision finale reste à l'appréciation d'un humain
  - Outils
    - Base d'intelligence artificielle
    - Machine learning

Piliers techniques de la sécurité de réseau

CORRECTION

- 4 – L'Active Directory
  - Appelé annuaire d'entreprise
  - Partie intégrante d'une attaque (souvent sous-estimé)
  - Les hackers ciblent le coeur de l'entreprise
    - Après avoir franchi les défenses périmétriques
  - Intérêt :
    - Accès aux comptes de l'ensemble de l'entreprise, administrateurs et grands patrons compris.
  - But
    - S'emparer des comptes à hauts-privilèges pour pouvoir (Ex : Ransonware)

Piliers techniques de la sécurité de réseau

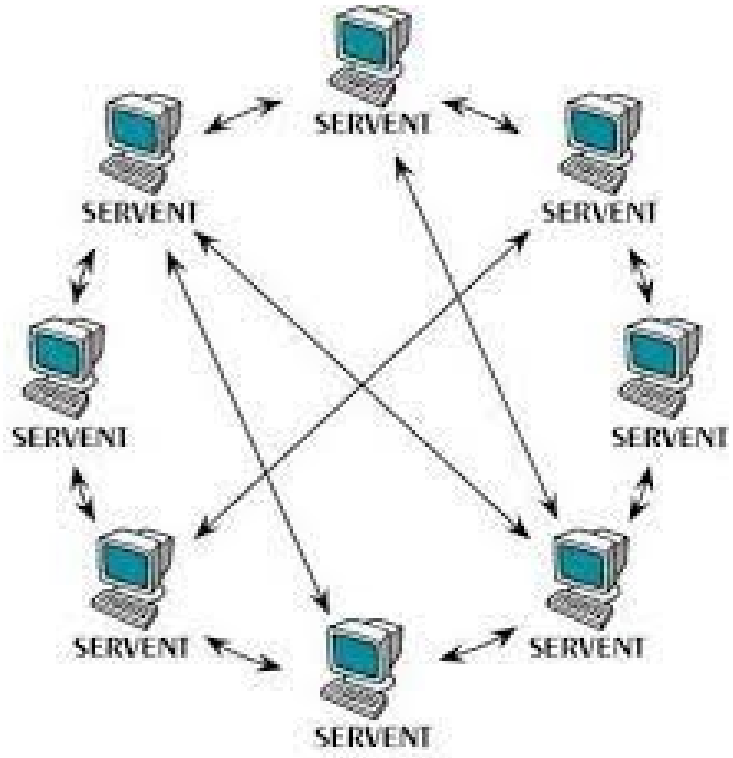
CORRECTION

- 5 – La sensibilisation des utilisateurs
  - Les failles sécuritaires modernes se situent toujours entre l'écran et le clavier
    - Chaque entreprise doit réduire les risques liés aux mauvais comportements des utilisateurs.
  - Solution
    - former pour éviter « clique à tout » grâce à des mises en situations, questionnaires ou vidéos interactives.
- La réalité est simple
  - Difficile d'être proactif en défense et de devancer les attaques

Piliers NON techniques de la sécurité de réseau

Correction

- 1- Limiter les accès Internet
  - Bloquant les services non nécessaires :
    - VoIP
    - Pair à pair (P2P)
    - Etc...



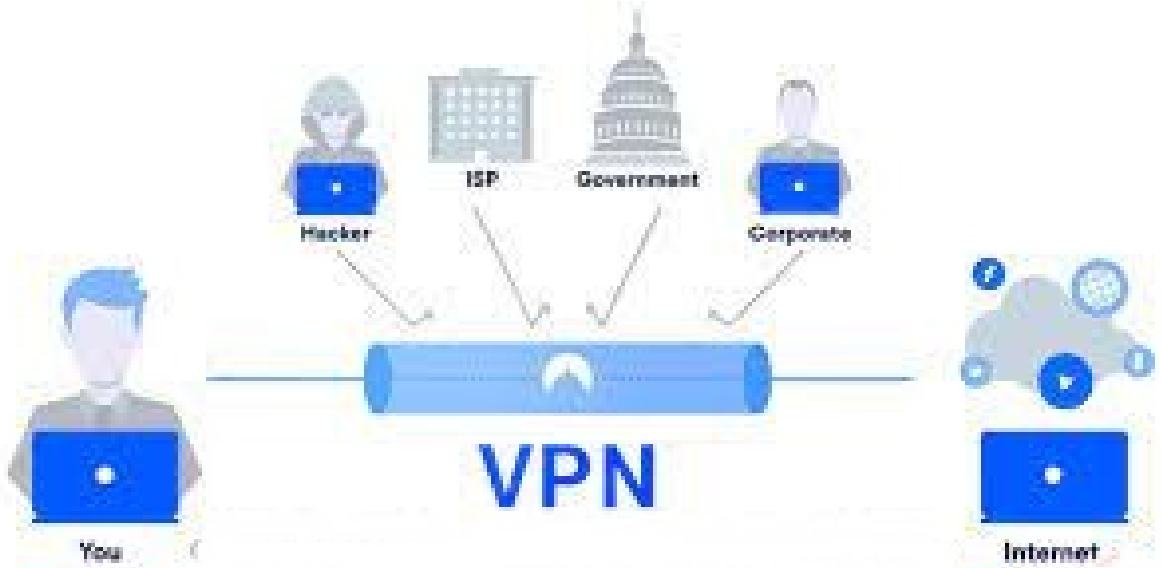
Piliers NON techniques de la sécurité de réseau

- 2 - Gérer les réseaux Wi-Fi
  - Utiliser un chiffrement
    - WPA-TKIP / WPA2-PSK
    - WPA2-AES / WPA2-AES-CCMP
    - Mot de passe complexe
  - Les réseaux ouverts aux invités
    - doivent être séparés du réseau interne

Piliers NON techniques de la sécurité de réseau

Correction

- 3 - Imposer un VPN pour l’accès à distance
  - Avec une authentification forte de l’utilisateur
    - carte à puce
    - Générateur de mots de passe à usage unique
    - Etc...



Piliers NON techniques de la sécurité de réseau

Correction

- 4 - Aucune interface d’administration
  - Non accessible directement depuis Internet
  - La télémaintenance doit
    - s’effectuer à travers un VPN

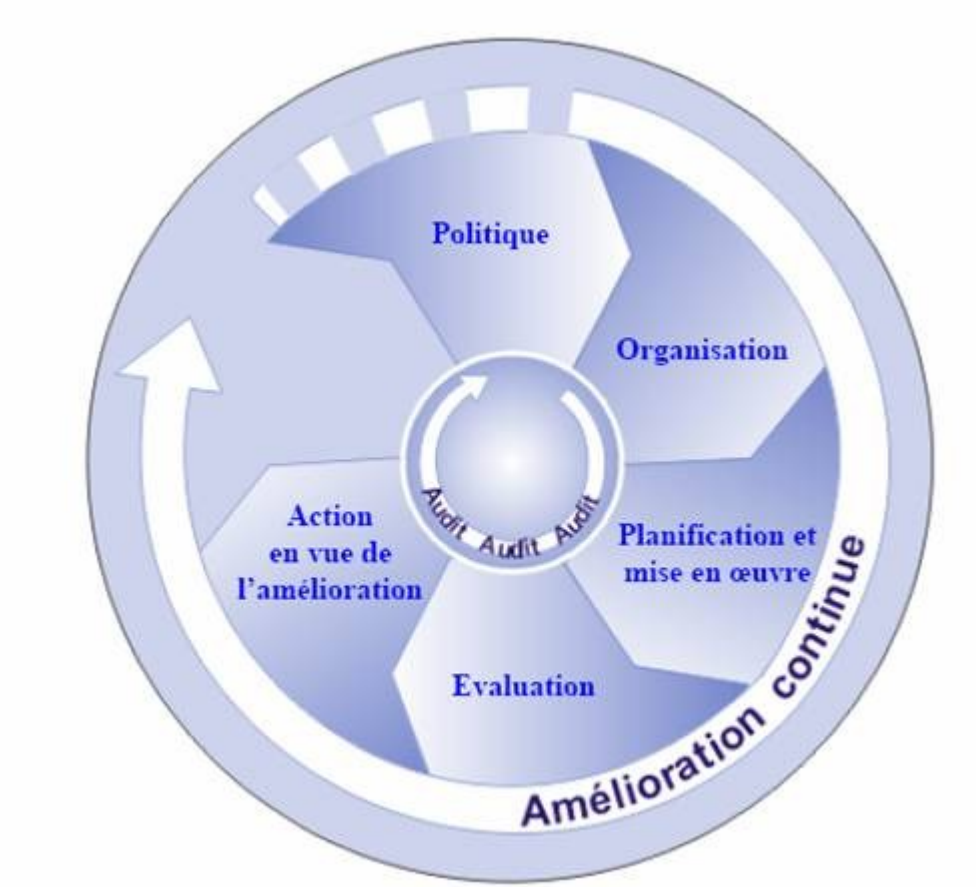
Piliers NON techniques de la sécurité de réseau

Correction

- 5 - Limiter les flux réseau
  - Au strict nécessaire
  - Filtrer les flux entrants/sortants
    - sur les équipements (pare-feu, proxy, serveurs, etc.)

Exemple :

Un serveur web utilise le HTTPS
→ Autoriser uniquement les flux entrants sur cette machine sur le port 443
→ Bloquer tous les autres ports.



- La sécurité au sein d'une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité

Introduction

- Les mesures de sécurité à mettre en place
  - dépendent de l'activité
  - de l'organisation
  - de la réglementation et des contraintes de son écosystème.
- Afin d'évaluer le niveau de sécurité attendue

  → Les questions à se poser ?

- Qu'est ce que je veux protéger ?
- De quoi je veux me protéger ?
- A quel type de risques mon organisation est exposée ?
- Qu'est ce que je redoute ?
- Quelles sont les normes qui s'appliquent à mon organisation ?

Comment gérer !!!

Politique

- Politique de Santé et Sécurité au Travail
- Participation des travailleurs

Organisation

- Responsabilité
- Compétences et formation
- Documentation relative à la SST
- Communication

Planification et mise en œuvre

- Examen initial
- Planification, élaboration et mise en œuvre du système
- Objectifs en matière de SST
- Prévention des risques

Action en vue de l'amélioration

- Action préventive et corrective
- Amélioration continue

Evaluation

- Suivi et mesure des résultats
- Enquête
- Audit
- Examen par la direction

Organisation

- L’organisation peut s’inspirer
  - De la famille de norme internationale ISO 27000
  - Des guides nationaux
    - ANSSI
    - CLUSIF
    - CNIL
  - Des politiques de sécurité en usage dans l’État
    - PSSIE
    - RGS
    - Etc
- pour mettre en place la sécurité.

Panorama des normes ISO 27000

- Permet à une organisation de mettre en œuvre
  - Améliorer le système de management de la sécurité :
    - Une certification ISO 27001 délivrée par un organisme certificateur accrédité garantie suite à un audit qu'une organisation a bien appliquée les exigences de la norme en matière de sécurité.
      - Cette certification est valable 3 ans, tous les ans un audit de contrôle est effectué.
    - Il peut être exigé à une organisation d'avoir cette certification pour accéder à certains contrats
      - par exemple un organisme payeur d'aides agricoles européennes.

Norme ISO 27001

- Permet à une organisation de mettre en œuvre
  - Améliorer le système de management de la sécurité :
    - Une certification ISO 27001 délivrée par un organisme certificateur accrédité garantie suite à un audit qu'une organisation a bien appliquée les exigences de la norme en matière de sécurité.
      - Cette certification est valable 3 ans, tous les ans un audit de contrôle est effectué.
    - Il peut être exigé à une organisation d'avoir cette certification pour accéder à certains contrats
      - par exemple un organisme payeur d'aides agricoles européennes.

SMSI 27001

- SMSI

  → Système de Management de la Sécurité de l'Information

- Démarche calquée sur ISO 9000 :
  - Plan
  - Do
  - Check
  - Act

Une entreprise
peut être certifiée ISO
27001

- Défini un périmètre réduit
- Politique de sécurité peu stricte.

Noter que la norme
N'impose pas de niveau minimum
de sécurité à atteindre.

Démarche 27001 (1/4)

Phase Plan	Phase Do	Phase Check	Phase Act

→ Fixer des objectifs et des plans d'actions :

- Identification des actifs ou des biens ;
- Analyse de risques ;
- Choisir le périmètre du SMSI :
  - Quel périmètre ?
    - C’est le domaine d’application du SMSI, son choix est libre
    - Doit être circonscrit
    - Ce sont toutes les activités pour lesquelles l’organisation exige de la confiance.
  - Quelle politique de sécurité ?
  - Quel niveau de sécurité : intégrité, confidentialité, disponibilité de l’information au sein de l’organisation ?

Démarche 27001 (2/4)

Phase Plan	Phase Do	Phase Check	Phase Act

→ Mise en œuvre

Et exploitation des mesures et de la politique

- Établir un plan de traitement des risques
- Déployer les mesures de sécurité
- Former et sensibiliser les personnels
- Détecter les incidents

en continu pour réagir rapidement

Démarche 27001 (3/4)

Phase Plan	Phase Do	Phase Check	Phase Act

→ mesurer les résultats issus des actions mises en œuvre

- Audits internes de conformité et d'efficacité du SMSI (ponctuels et planifiés)
- Réexaminer l'adéquation de la politique SSI avec son environnement
- Suivre l'efficacité des mesures et la conformité du système
- Suivre les risques résiduels

Démarche 27001 (4/4)

Phase Plan	Phase Do	Phase Check	Phase Act

→ Planifier et

suivre les actions correctrices et préventives

Avantages (1/2)

- Mise en œuvre des objectifs et des mesures de sécurité
- Audits réguliers
  - Permettent le suivi entre
    - Les risques initialement identifiés,
    - Les mesures prises et les risques nouveaux ou mis à jour.
  - Objectif : mesurer l'efficacité des mesures prises
- Sécurité
  - Amélioration continue de la sécurité

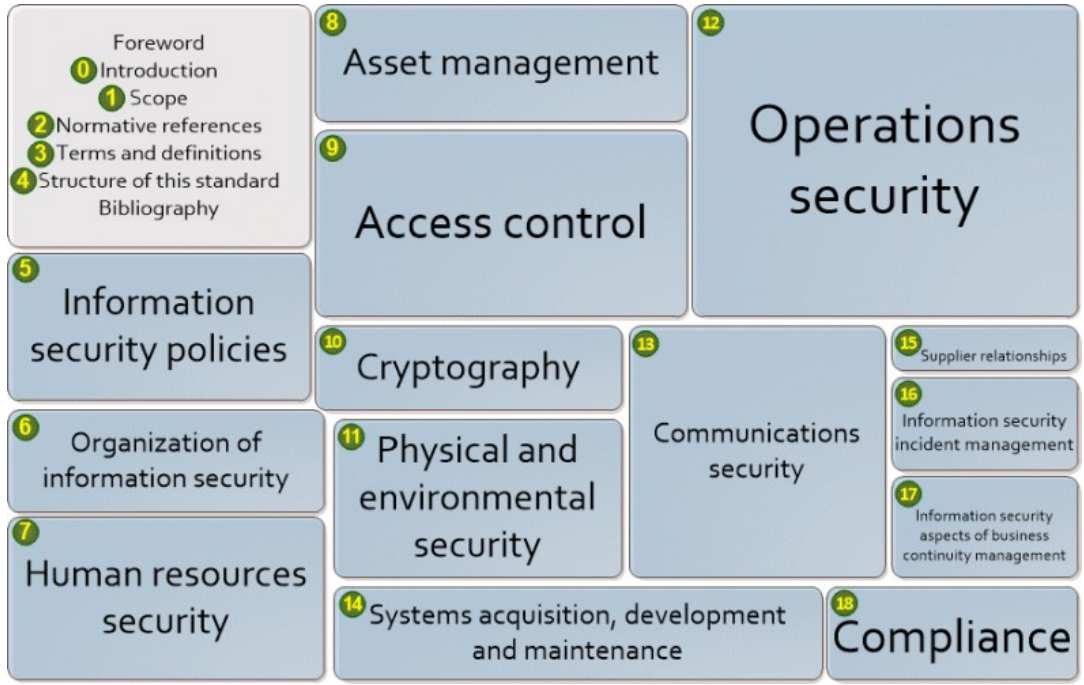
    → Un niveau croissant de sécurité et de maturité en SSI

Avantages (2/2)

- Meilleure maîtrise des différents risques
- Élimination des mesures de sécurité non usitées
- Amélioration
  - Confiance des associés, partenaires & clients ;
- Référentiel international
  - Facilite les échanges
- Indicateurs clairs et fiables
  - Produisant des éléments de pilotage financier pour les dirigeants.

Norme ISO 27002

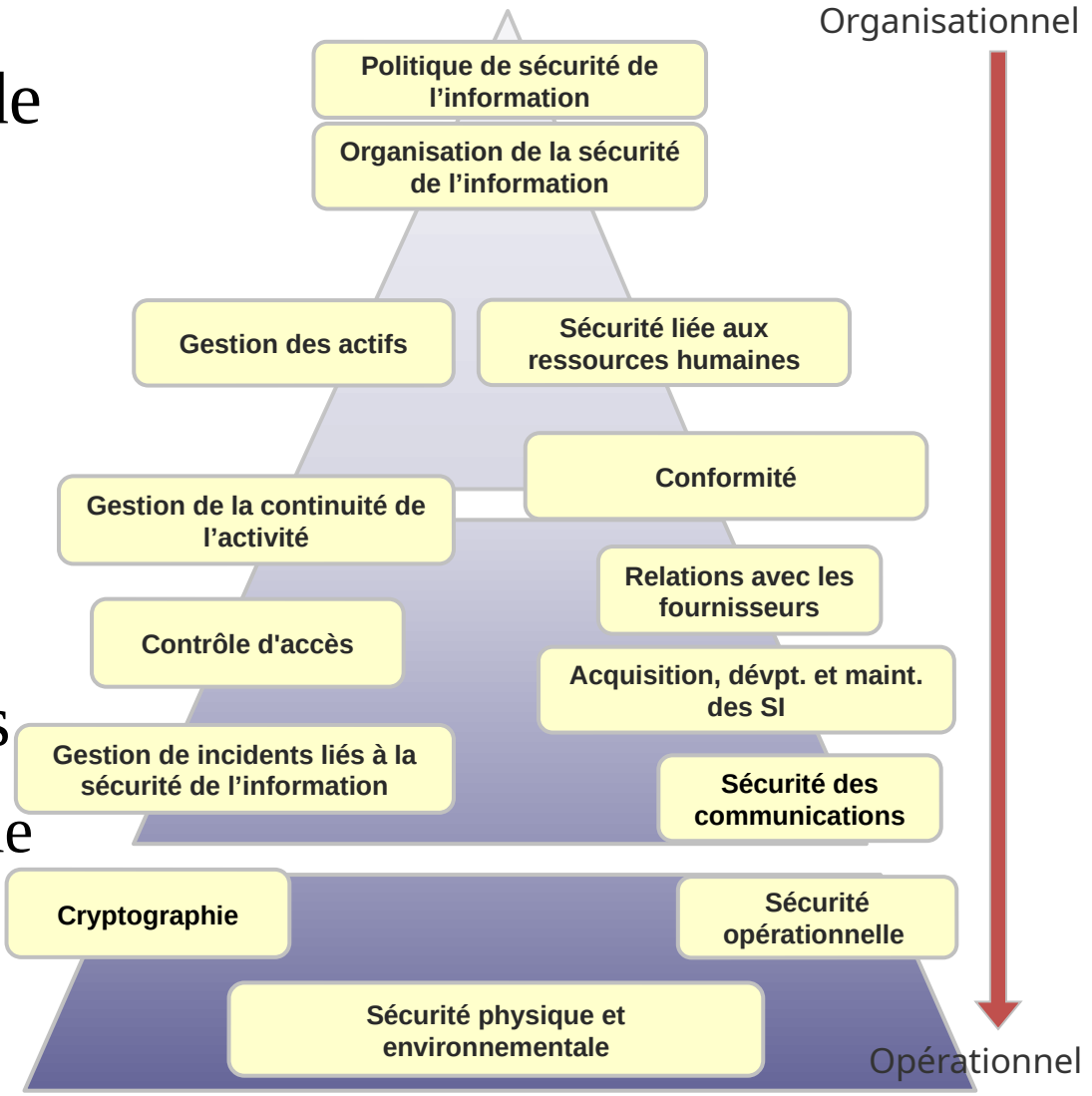
- Code de bonnes pratiques
  - pour le management de la sécurité de l'information
- Définit un ensemble de « bonnes pratiques » en matière de sécurité répartie en plusieurs chapitres, l'organisation dispose :
  - d'un référentiel de mise en œuvre ;
  - d'une « check-list » en cas d'audit.



Bonnes pratiques

ISO 27002

- Constitue un code de bonnes pratiques.
- Composée de 114 mesures de sécurité
- Regrouper en 14 chapitres
- Couvre les domaines
  - Organisationnels
  - Techniques
- L’ensemble de ces domaines
  - Avoir une approche globale de la sécurité des S.I.



Contrôle d’accès : Exemple

ISO 27002

- L’accès aux fichiers/répertoires
  - Doit être restreint conformément
    - aux politiques de contrôle d’accès :
      - Seuls les personnes autorisés doivent pouvoir accéder
        - A un répertoire précis
- Les propriétaires de l’information
  - Doivent vérifier les droits d’accès
    - A intervalles réguliers :
      - Le responsable doit contrôler les droits d’accès au répertoire contenant les épreuves des futurs examens/concours pour s’assurer qu’il n’y a pas d’étudiants qui auraient été rajoutés.

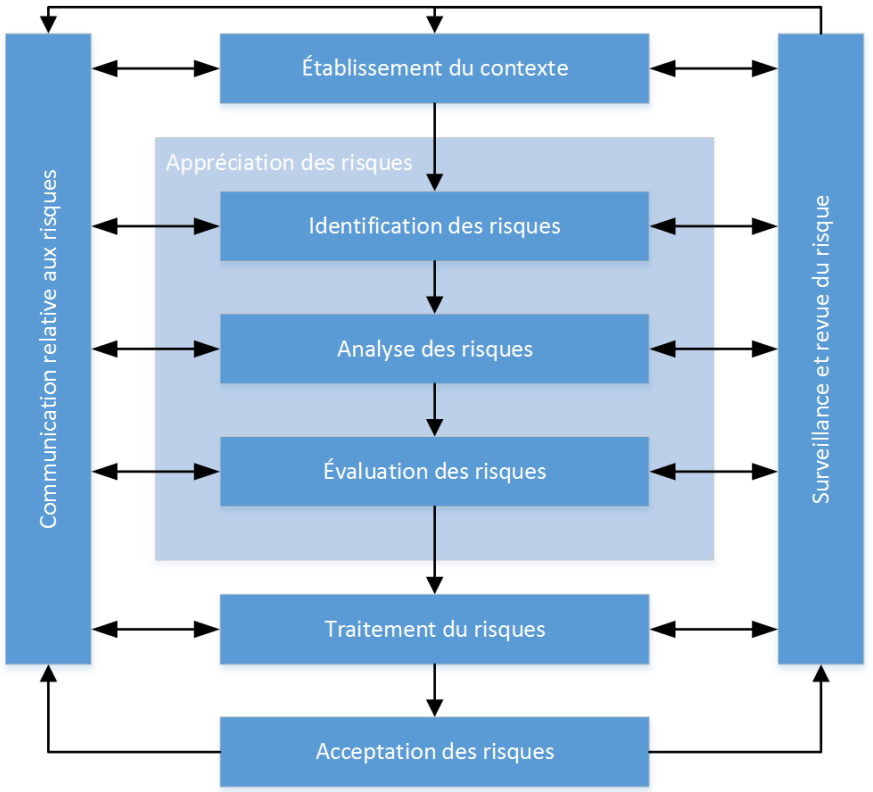
Sécurité opérationnelle : Exemple

ISO 27002

- L’installation et la configuration de logiciels doivent être encadrés :
    - Seuls les administrateurs doivent pouvoir installés un logiciel sur un poste.
- Des sauvegardes doivent êtres régulièrement effectuées et testées :
    - Un espace de sauvegarde des données peut être mis à disposition des utilisateurs.

Norme ISO 27005

- Définit des lignes directrices relatives
  - A la gestion des risques de sécurité dans une organisation.
- Une organisation peut s'appuyer
  - Processus de gestion de risques
    - pour intégrer la sécurité.



Gestion des risques

- La norme 27005 présente une démarche :
  - Établissement du contexte de l’analyse des risques
  - Définition de l’appréciation des risques SSI
  - Choix pour le traitement du risque SSI
  - Acceptation du risque
  - Communication et concertation relative aux risques SSI
  - Surveillance et revue du risque en SSI

Avantages

- Définit une démarche rationnelle
  - qui a donné lieu à des méthodes qui fonctionnent
- Grande souplesse
  - utilisée en toutes circonstances, surtout lors des changements
- Pragmatique et utilisable seule
  - Peut aussi bien convenir aux petites organisations

Limites

- L'organisation doit définir sa propre approche
- Méthodes nécessitant souvent de la formation et non adaptables à toutes les situations
- Dépendance vis-à-vis de la cartographie du SI :
  - Profondeur, étendue, etc.
- Tendance à l'exhaustivité
- Accumulation de mesures techniques sans cohérence d'ensemble

Classification des informations (1/2)

- La classification selon la confidentialité des informations
  - Permet de définir les mesures de protection appropriées

    pour chaque type d'information.

	Explication	Exemple	Risque
Accès libre	Tout le monde peut y accéder	Informations publiées sur le site internet	Aucun
Accès à l'organisation	Seul le personnel de l'organisation est autorisé à accéder à l'information	Nom, adresse des partenaires et fournisseurs de l'organisation	Atteinte à l'image, gêne passagère
Diffusion limitée	Au sein de l'organisation, seul un groupe de personnes est autorisé comme les membres du même projet	Plan technique d'un nouveau laboratoire ; Listes der personnes admissibles avant publication officielle…	Situation à risques ; pertes financières acceptables
Confidentiel	L'information est accessible à une liste très restreinte d'utilisateurs à titre individuel	Contenu des brevets déposés ; Recherche en cours ; N° de sécurité sociale et noms…	Pertes financières inacceptables, poursuites judiciaires

Classification des informations (2/2)

- Sur la base des niveaux de confidentialité définis

  les mesures suivantes peuvent être implémentées :

  - Une politique de gestion des informations est définie :
    - Création d'un modèle de document indiquant le niveau de confidentialité
    - Sensibilisation du personnel et des partenaires à cette politique
  - Les informations de niveau « Confidentiel » doivent être :
    - envoyées par mail de manière chiffrée et le mot de passe communiqué par SMS aux destinataires ;
    - stockées localement dans des conteneurs chiffrés.
  - Les informations de niveau « Diffusion limitée »
    - Doivent être échangées au travers
      - Un système documentaire collaboratif
      - ayant des accès nominatifs contrôlés

Gestion des ressources humaines

Avant embauche	Pendant l'embauche	Fin contrat de travail

- Avant embauche :
  - Sélection des candidats et interviews ;
  - Vérification du CV (contacter les anciens employeurs, vérifier les diplômes, certifications…) du candidat ;
  - En fonction de la sensibilité du poste, un extrait de casier judiciaire peut être demandé.

Gestion des ressources humaines (2/

Avant embauche | **Pendant l’embauche** | Fin contrat de travail

- Pendant l’embauche :
  - Fourniture des accès logiques (création de comptes utilisateurs, accès aux répertoires nécessaires…) et physiques (badges) adaptés à la fonction ;
  - Sensibilisation aux politiques et procédures internes de l’organisation ;
  - Sensibilisation régulière à la sécurité adaptée aux fonctions ;
  - Processus disciplinaire en cas de non respect.

Gestion des ressources humaines

Avant embauche	Pendant l'embauche	Fin contrat de travail

- Au terme du contrat de travail :
  - Retrait des accès et restitution du matériel fourni (badge, ordinateur, …).

A retenir

- Une politique de sécurité
  - doit être adaptée à l'organisme et à ses évolutions
- La sécurité ne s'improvise pas
  - Nécessite des professionnels ;
- Les normes sont une aide
  - Mettre en œuvre une démarche d'amélioration continue de la sécurité
- Les normes par nature ne délivrent pas
  - un niveau de sécurité
- Les normes ne prennent pas en compte
  - toute la sécurité des systèmes d'information.

https://school.hello-design.fr

5A

- La sécurité au sein d’une organisation
- La sécurité dans les projets
- Difficultés liées à la prise en compte de la sécurité

Introduction (1/

- Il s’agit de bien distinguer :
  - la sécurité du système d’information qui est un des objets du projet ;
  - et la sécurité du projet en lui-même (diffusion et traitement des informations).
- Concernant la sécurité du SI en lui-même :
  - Toute activité étant gérée en mode projet

    → Une bonne intégration de la sécurité dans l’organisation

    nécessite l’intégration de la sécurité dans chaque projet

    dans le respect de la réglementation
  - Isoler les traitements de données sensibles

    → Au sein de projet pour avoir

    une meilleure maîtrise des risques et des mesures de sécurité

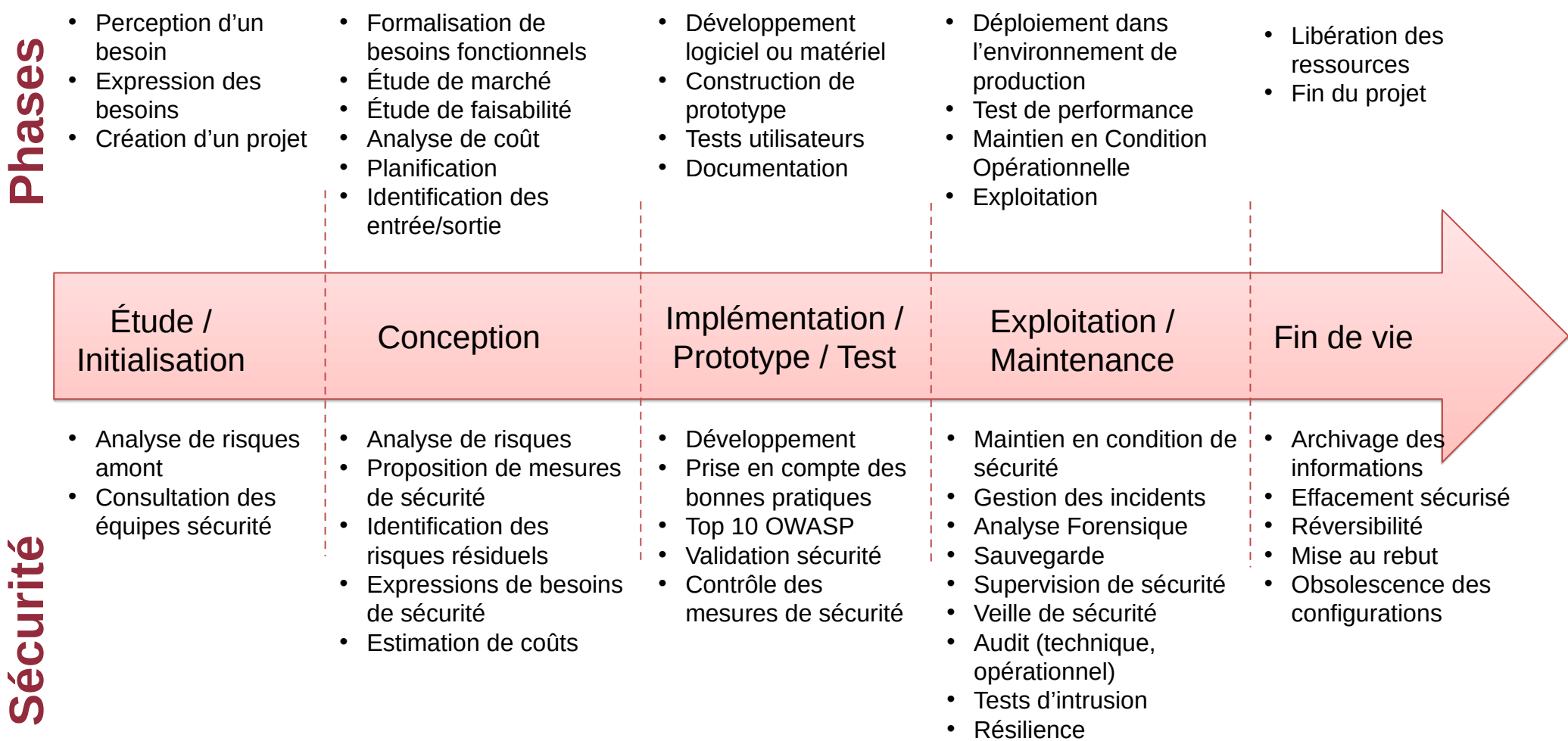
    à mettre en œuvre pour réduire ces risques.

Introduction (2/

- La sécurité doit être prise en compte dans toutes les étapes d'un projet :
  - Application de la démarche d'amélioration continue
  - Respect des impératifs et des contraintes notamment juridiques et réglementaires
  - Responsabilisation
    - Acteurs
    - Documentations
    - Gestion du temps.

Exemple

- Intégration de la sécurité dans le cycle de vie d'un projet



Exemple (1/2)

- Projet de développement de site Web :
  - L’audit de sécurité fait un constat :
    - Les versions de composants logiciels utilisés
      - sont obsolètes et vulnérables
    - La base de données n’a pas été correctement isolée
      - Les tables ont été créées à l’intérieur d’une autre base de données à accès public
    - La politique de gestion de mots de passe n’est pas conforme aux bonnes pratiques :
      - création de mots de passe faibles
      - stockage de mots de passe en clair…
    - Le niveau de disponibilité attendu pour ce site
      - ne peut être assurer avec l’infrastructure existante.

Exemple (2/2)

- Projet de développement de site Web :
  - Conséquences :
    - Besoin de rachats de licences logicielles
      - coût supplémentaire
    - Recréation de la base de données
      - sur un espace dédié correctement protégé
    - Re-développement des modules
      - de gestion des mots de passe : coût supplémentaire
    - Modification de l’infrastructure
      - pour assurer le niveau de disponibilité requis

Sécurité prise en compte en fin de déploiement

- Exemple d'un projet de construction d'une nouvelle salle devant hébergée les serveurs de l'organisation :
  - L'audit de sécurité fait le constat que :
    - Les baies de stockage des serveurs ne se ferment pas à clé
    - Pas de mécanisme de contrôle d'accès (lecteur de badge) prévu tracer les accès
    - Pas de redondance (alimentation, accès de télécommunications) des équipements
    - Aucune alarme anti-intrusion ou incendie n'est prévue
    - L'arrivée de câbles dans la salle est exposée à des actes de malveillances
    - La salle est construite en zone inondable.
  - Conséquences :
    - Rachat de matériel et d'équipements => coût supplémentaire
    - Re-câblage de la salle, et travaux de génie civil à prévoir
    - Relocation de la salle ou reconstruction => coût supplémentaire très importante.

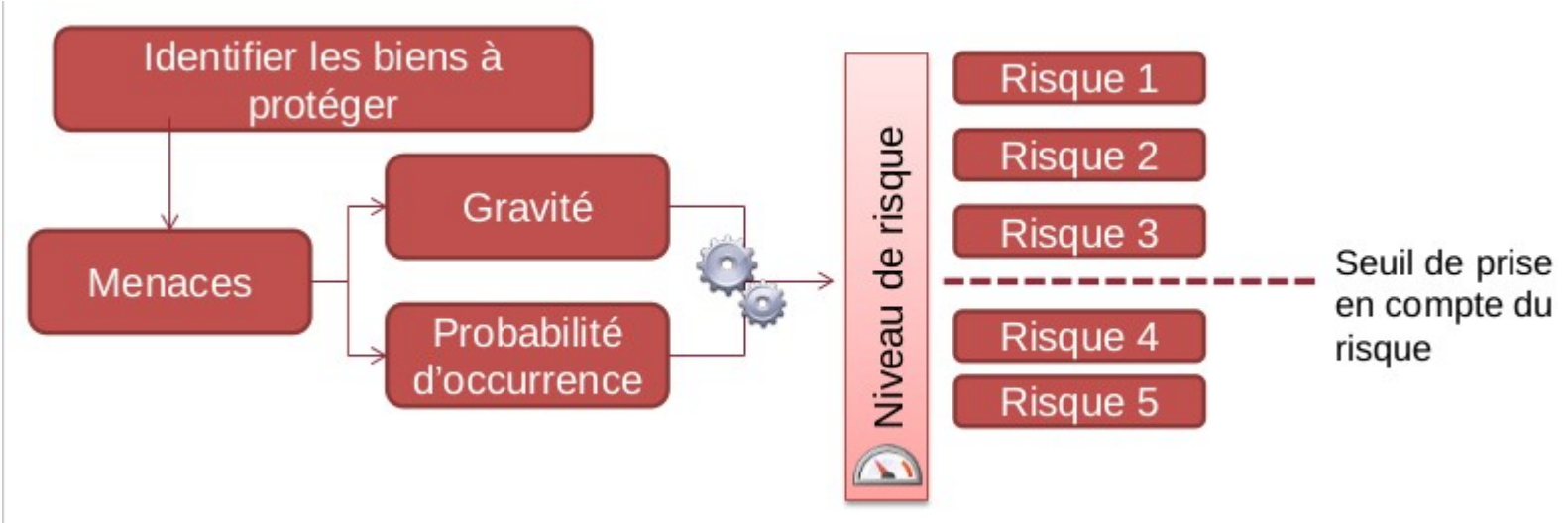
L’approche par l’analyse et le traitement du risque

- L’analyse de risques doit être effectuée en amont du projet
  - mais doit aussi évoluer au fur et à mesure de l’exploitation du système
    - Analyse de risque dynamique dans la supervision du système (SOC)
    - Fonction de l’évolution des risques
      - évolution des vulnérabilités, des menaces, du système d'information
- L’analyse de risque consiste à :
  - identifier les biens à protéger
  - analyser de la fréquence et la gravité du danger pour évaluer la criticité du risque
  - établir une hiérarchisation des risques : fréquence vs gravité
  - établir un seuil d’acceptabilité pour chacun de ces risques
    - seuil au-delà duquel le risque doit être pris en compte par les mesures de sécurité.
  - identifier des mesures de sécurité
- Les mesures ainsi identifiées peuvent constituer
  - un cahier de charges sécurité

    pour le projet qui soit réalisé en interne ou externalisé

L’approche par l’analyse et le traitement du risque

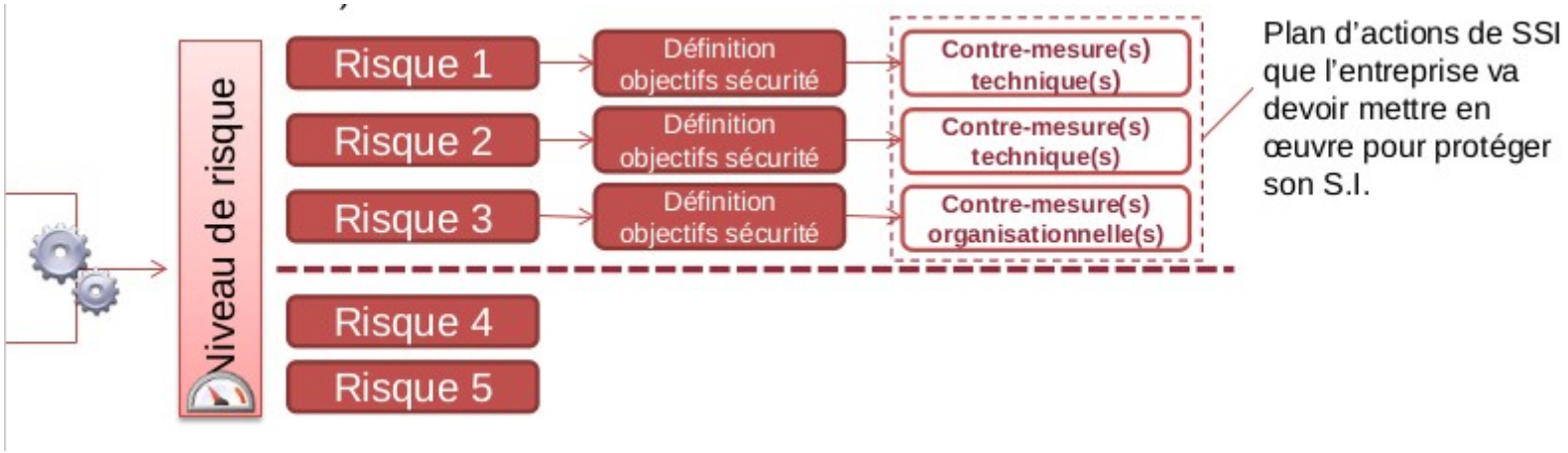
- Une démarche d’analyse de risque peut être schématisée ci-dessous :



- La hiérarchisation des risques permet de déterminer les risques qui
  - doivent absolument être traités et donc réduits par des mesures
  - ceux qui sont acceptables et avec lesquels le système peut exister

L’approche par l’analyse et le traitement du risque

- Pour les risques dont le niveau est supérieur au seuil de prise en compte :
  - Définir les objectifs de sécurité ;
  - Définir les mesures techniques et organisationnelles qui vont permettre d’atteindre ces objectifs.
- Pour les risques dont le niveau est inférieur au seuil de prise en compte :
  - un risque résiduel est le risque subsistant après le traitement de risque
    - Exemple : le coût pour compenser ce risque est trop élevé par rapport au risque encouru



L’approche par l’analyse et le traitement du risque

- Une analyse de risque peut être
  - Complexe
  - Nécessite rigueur et méthode
  - Il faut notamment trouver le bon niveau abstraction.

Exemples

- Méthodes d’analyses de risque compatibles
  - Lignes directrices de l’ISO 27005
    - EBIOS
      - Expression des Besoins et Identification des Objectifs de Sécurité

      → développée par le Club EBIOS auquel participe l’ANSSI, l’Agence nationale de la sécurité des systèmes d’information
    - MEHARI :
      - Méthode Harmonisée d'Analyse de Risques

      → développée par
        - le CLUSIF, Club de la Sécurité de l’Information Français
    - OCTAVE :
      - Operationally Critical Threat, Asset, and Vulnerability Evaluation

      → développée par l’Université de Carnegie Mellon.

Plan d’actions SSI

- Le défi vis-à-vis de la mise en place des mesures de sécurité

  est asymétrique entre « attaquer » et « défendre » :

  - L’attaque peut réussir par l’exploitation d’une seule vulnérabilité ;
  - Tandis que la défense doit prendre en compte l’ensemble du système.

- Un plan d’action des mesures de sécurité à mettre en place

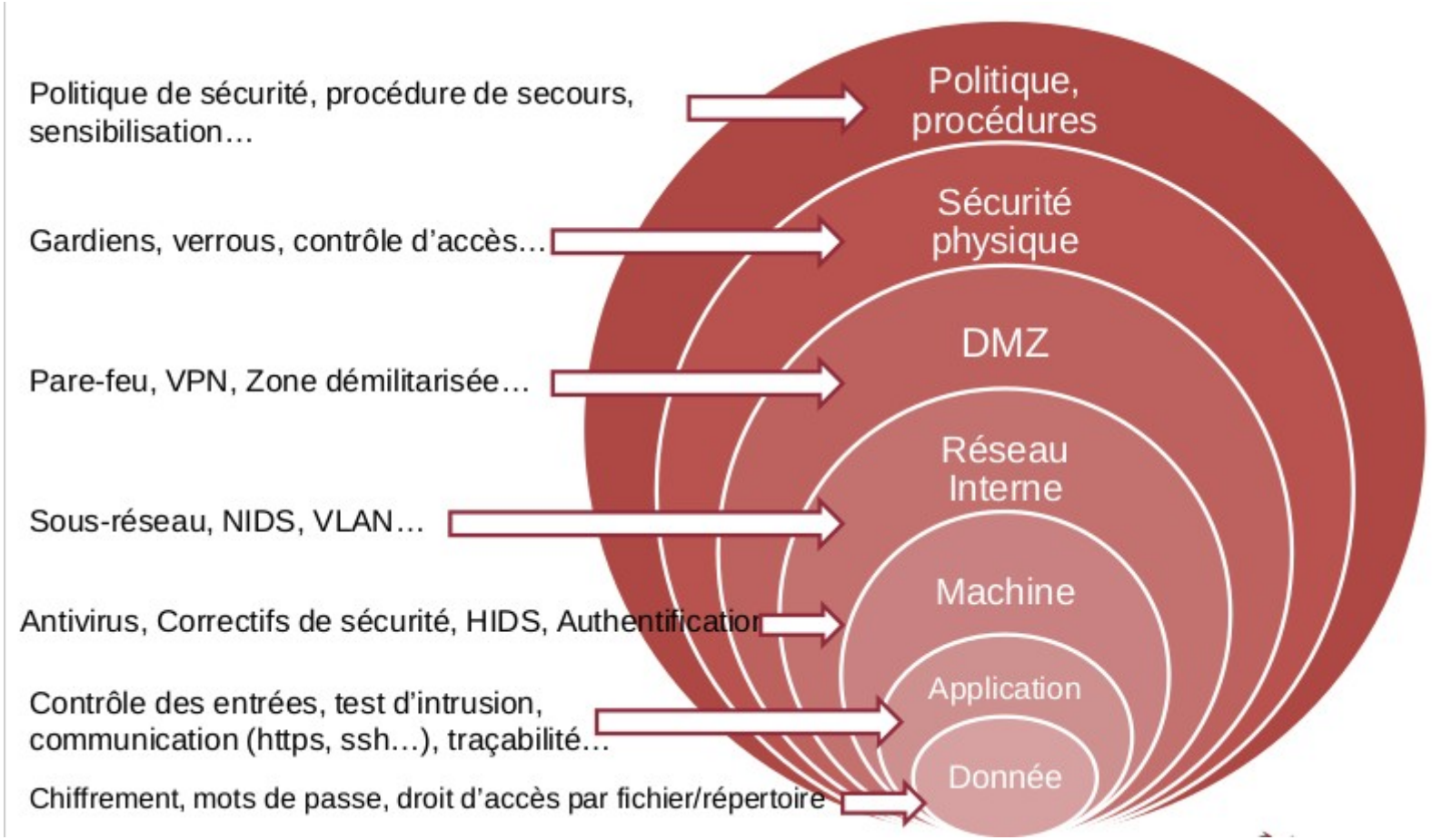
  à l’issue de l’analyse de risques devrait respecter le principe de « défense en profondeur » qui recommande :

  - D’avoir plusieurs lignes de défenses indépendantes
  - que chaque ligne constitue une barrière autonome contre les attaques
  - que la perte d’une ligne de défense implique

    qu’on passe à un niveau de défense plus fort.

- Les objectifs de la défense en profondeur sont :
  - prévenir, bloquer, limiter, détecter, alerter, réagir, réparer.

Plan d’actions SSI



En résumé

- La sécurité des systèmes d'information
  - un élément indispensable d'un projet
- une sécurité globale et cohérente
  - et non une accumulation de mesures et de produits de sécurité
- une politique de sécurité réaliste et pragmatique
- un élément clé :
  - la connaissance du système d'information (cartographie)

    et de son niveau de sécurité (contrôle, audit)
- une difficulté et une nécessité :
  - le maintien en condition de sécurité du système d'information
- un accroissement des besoins de sécurité :
  - besoin en compétences et en professionnels

https://school.hello-design.fr

5B

La suite de la Session 5 ???

- La suite de cette partie
  - Rendez vous la semaine prochaine

Session 5 - Partie 2

TP 5 : Brainstorming
En Groupe - En classe

Rendez-vous au prochain cours

- Merci de votre attention