Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

La défense en profondeur appliquée à la sécurité des systèmes d'information

Bureau conseil de la DCSSI
Conseil.dcssi@sgdn.pm.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Analyse des contextes

	Militaire	Industriel	SSI
Surprise	**Toujours** recherchée fait partie de la manœuvre	Élément à réduire au maximum	Toujours de nouvelle forme d'attaque. La défense n'a pas **l'initiative**
Renseignement	Il permet de diminuer l'incertitude sur les actions « ennemies » en infirmant ou confirmant les hypothèses. Il est indissociable de la **planification**.		
Coopération entre lignes	**Synergie** systématiquement recherchée. ex combat aéroterrestre	**Indépendance** des lignes vis à vis des menaces	Une ligne est fortement liée à une menace
Origine des menaces	« L'ennemi » agit dans toute la profondeur du dispositif Notion de défense immédiate, rapprochée et éloignée.		

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Enseignements issus du monde militaire …

- ✓ Le **renseignement** constitue la première ligne de défense : il n'y a pas de défense sans efficace sans source de renseignement.
- ✓ Les lignes de défense doivent être **ordonnées** et **coordonnées**: combinaison de défense par le feu indirect (l'artillerie) et le feu direct (les chars).
- ✓ La perte d'une ligne doit **affaiblir l'attaque :** au moins indirectement par l'acquisition de renseignement.
- ✓ La défense n'exclue pas des actions **offensives** comme une contre attaque.
- ✓ Une ligne de défense doit être **complète** : elle intègre des parades à tout type d'attaque. Elle s'intègre au sein d'une **planification**.
- ✓ Aujourd'hui ce concept est dépassé car la doctrine d'emploi des forces est orientée vers la prévention et la projection

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

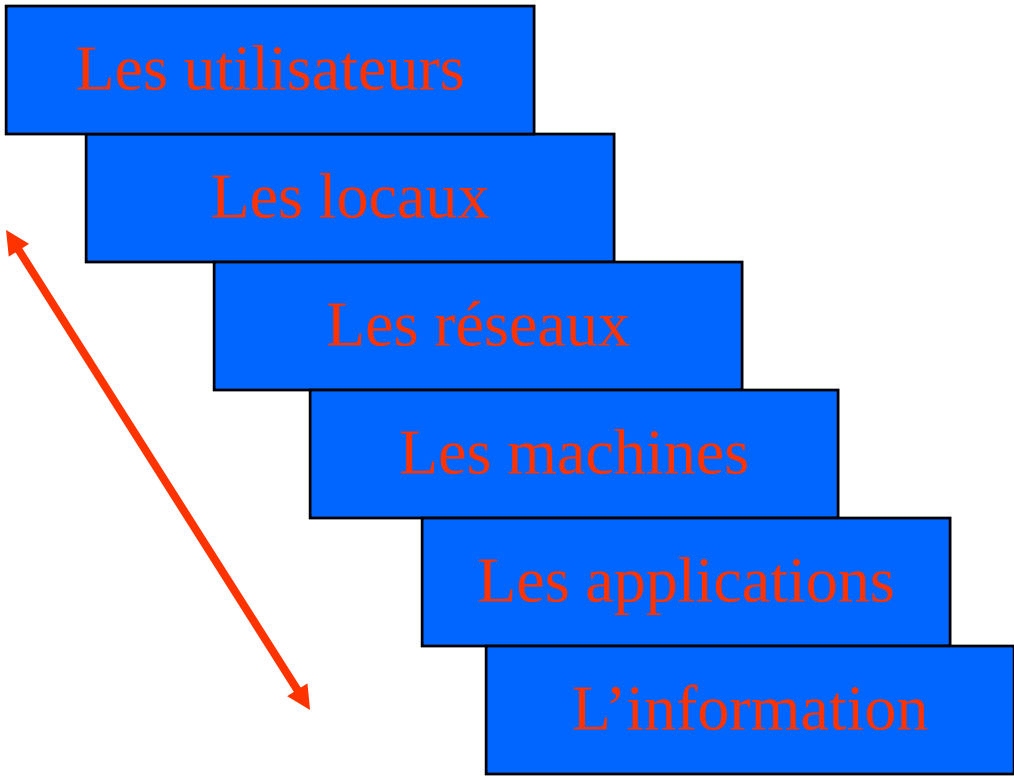
Enseignements issus du monde civil

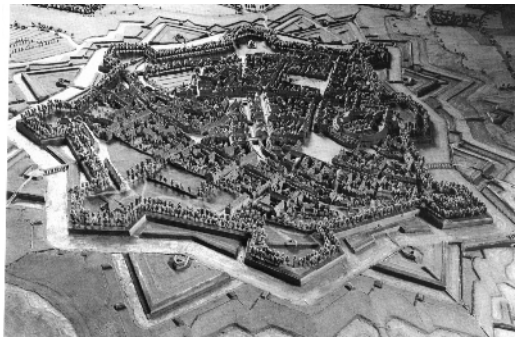
- ✓ La définition des objectifs est un pré-requis
- ✓ L'analyse des risques est ensuite conduite (approche déterministe ou probabiliste) afin de déterminer les barrières
- ✓ Les incidents de sécurité sont gradués sur une échelle globale :
  - ➢ Connue et reconnue
  - ➢ Permet de communiquer sur la défense
  - ➢ Permet de déterminer objectivement le niveau de gravité d'un événement
- ✓ Une sûreté se démontre par une approche qui peut être déterministe : scénarios enveloppes et/ou analyse par éléments défaillants

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Les principes généraux

- **La défense doit être globale**
  - aspects organisationnels
  - aspects techniques
- **La défense doit être coordonnée**
  - alerte
  - corrélation
- **La défense doit être dynamique**
  - capacité de réaction
  - planification des actions
  - échelle de gravité
- **Chaque dispositif dispose de 3 fonctions de sécurité**
  - protection
  - détection
  - réaction
- **La défense doit être démontrée**



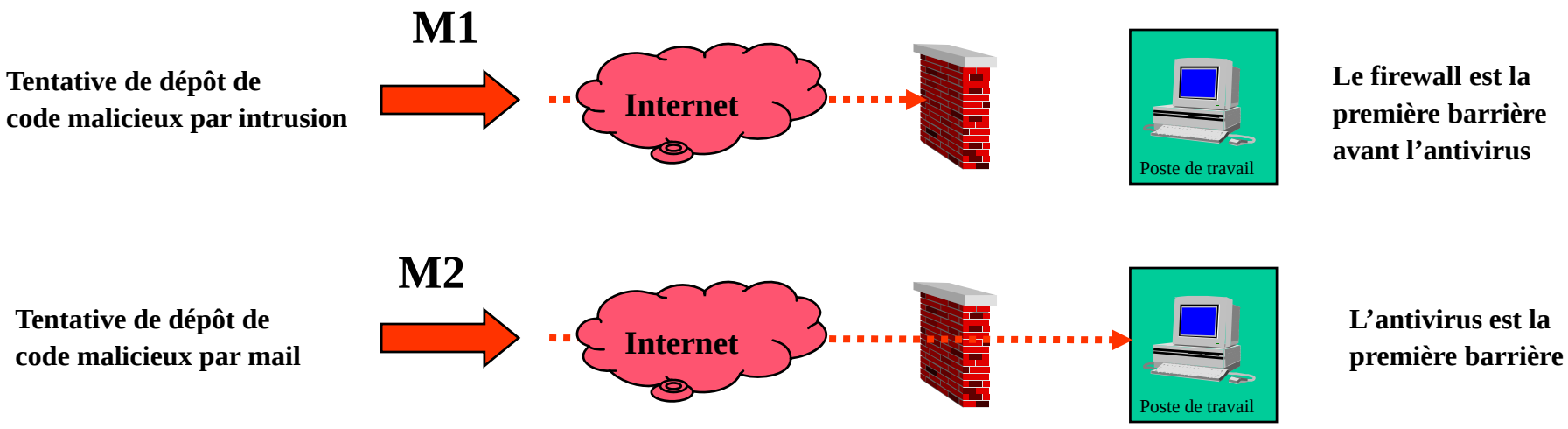


Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Définition du concept (1/4)

Un constat : l'insuffisance de la notion de barrière

- une barrière est uniquement liée à la composante protectrice (contingentement, cloisonnement)
- une barrière est trop dépendante de la menace



On parlera donc de lignes de défense corrélées à des niveaux de gravité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Définition du concept (2/4)

✓Gravité

La **gravité** d'un événement de sécurité mesure l'impact de l'événement en fonction de la criticité du bien menacé et du **nombre de lignes de défense restantes.**

✓Barrière

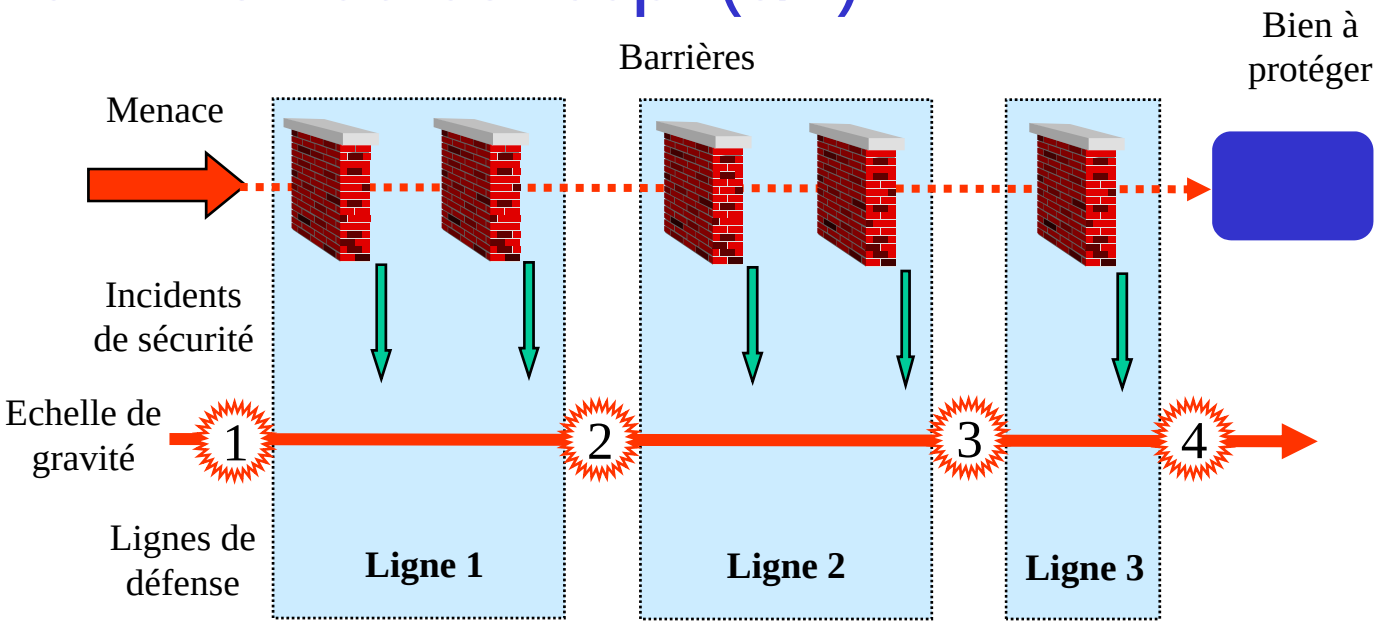
Une **barrière** est un moyen de sécurité capable de protéger une partie du système d'information contre au moins une menace. Une barrière peut être humaine, procédurale ou technique, statique ou dynamique, manuelle ou automatique. Elle doit bénéficier d'un moyen de **contrôle** de son état.

✓Ligne défense

Une **ligne de défense** est un ensemble de barrières, par scénario ou famille de scénarii, dont le franchissement provoque un changement de niveau de gravité.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Définition du concept (3/4)



✓Déterminer les barrières à mettre en place en fonction des menaces et des biens à protéger (par approche inductive et déductive)

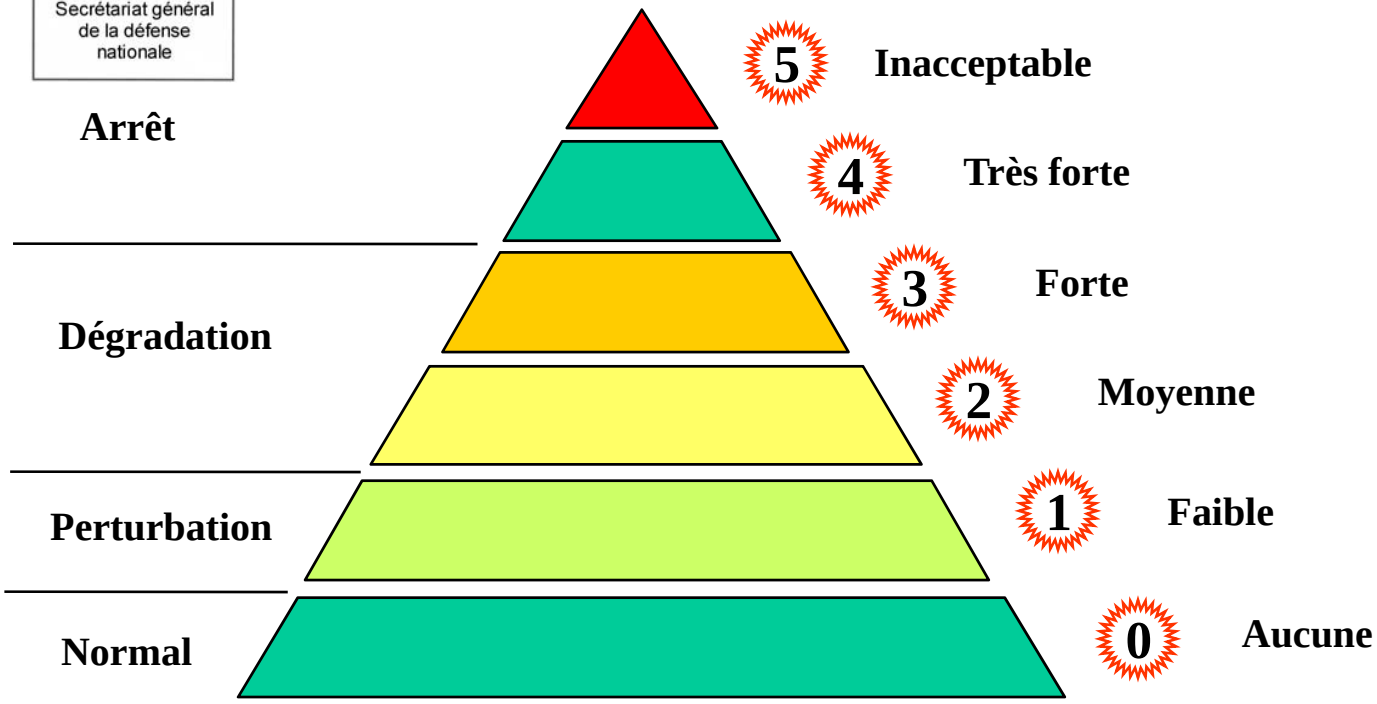
✓Déterminer le niveau de gravité des incidents de sécurité déclenchés par le franchissement des barrières

✓La ligne de défense regroupe les barrières à franchir ayant un niveau de gravité identique (complémentarité des moyens)

✓ Le nombre de lignes dépend de la gravité des événements redoutés (aspect cumulatif des défenses)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Echelle de gravité SSI



Inacceptable	Système de vente indisponible 1 h
Très forte	Système de réception des commandes indisponible 2 h
Forte	Système de communication en magasin indisponible 1 h
Moyenne	Communication avec comptabilité indisponible 3 h

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Définition du concept (4/4)

*La **défense en profondeur** du SI est une défense globale coordonnant plusieurs lignes de défense.*

Elle s'appuie sur une gestion des risques, un système de renseignement, une planification des réactions et l'enrichissement permanent grâce au retour d'expérience.

Elle poursuit un double but :

- *renforcer la protection du SI en démontrant la qualité du dispositif*
- *donner un moyen de communication fort permettant aux décideurs et aux utilisateurs de prendre conscience de la gravité des incidents de sécurité.*

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

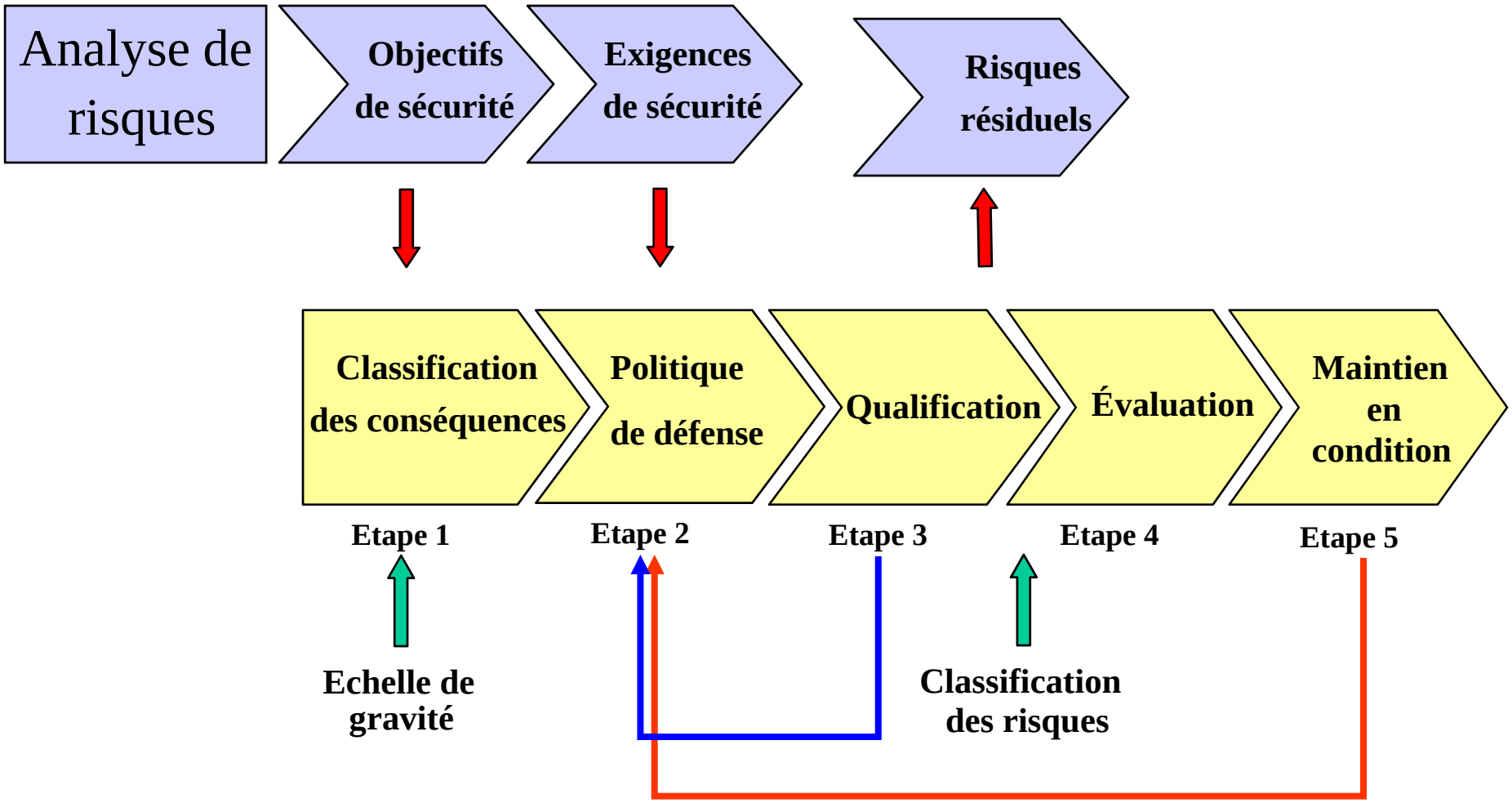
Méthode associée au concept

La méthode comprend trois volets principaux :

- ✓ construction de la défense à partir des biens à protéger et des techniques de défense ;
- ✓ détermination des points de contrôle (permettre de piloter la défense, l'évaluer, etc.) ;
- ✓ évaluation et qualification à partir des méthodes d'attaques.

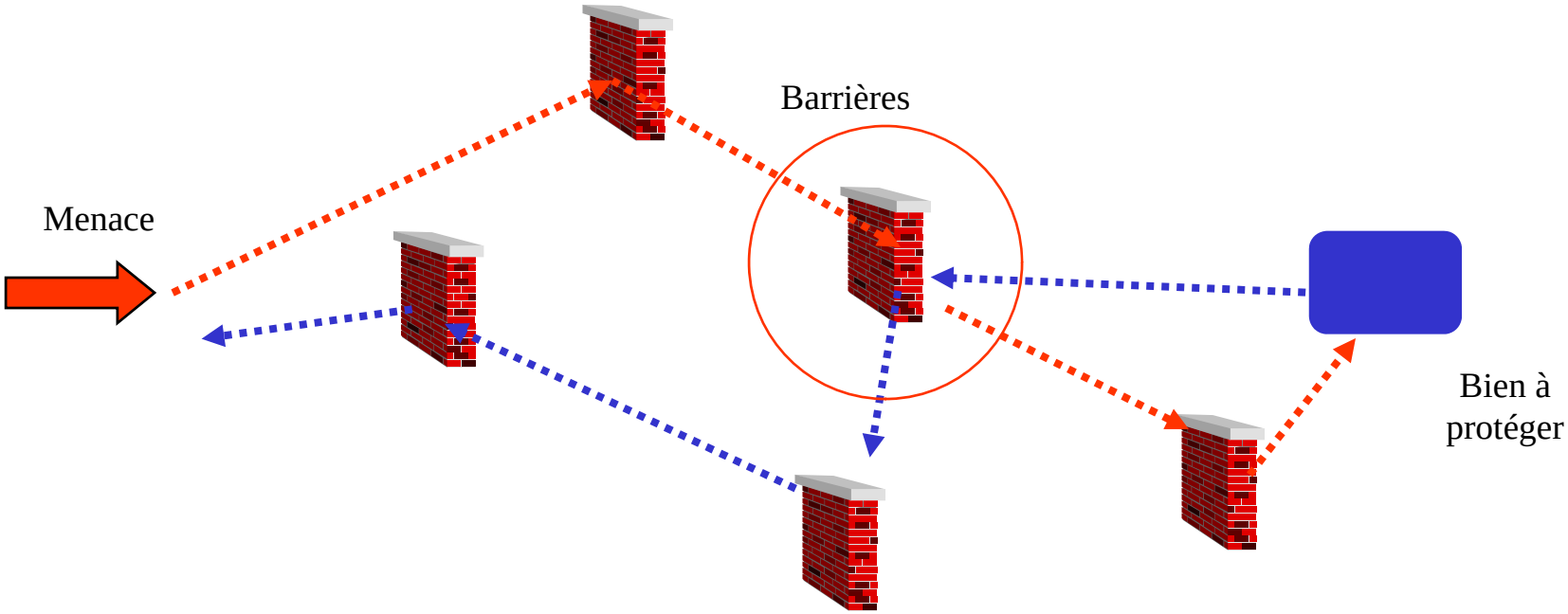
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Étapes de la méthode



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Étape 2 : détermination des barrières



Approche inductive : de la menace vers le bien

Approche déductive : du bien vers la menace

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Étape 3: qualification

- ✓ La qualification se fait selon deux approches
  - ➢ formelle : les principes de la défense en profondeur sont bien respectés. On se rapproche d'une démarche qualité.
  - ➢ démonstrative au travers des scénarios et des composants
- ✓ En fin d'étape les incidents sont classés par niveaux de gravité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Étape 3: qualification

- ✓ Éléments pour la qualification:
  - Il y a au moins 3 lignes de défense par bien
  - Le nombre de lignes de défense est adapté à la criticité du bien et au risque
  - La gravité d'un incident dépend plus des moyens de défense restants que de ceux qui ont été franchis
- ✓ Conduite de la démonstration :
  - Détermination de scénarios « enveloppes » et analyse de la défense
  - Analyse par composant défaillant : on postule un incident de sécurité et une défaillance aléatoire d'un autre composant situé entre l'incident et l'événement redouté pour analyser la protection restante et vérifier qu'elle est suffisante

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Conclusion : axe de progrès avec EBIOS

- ✓ Propositions d'avancées pour EBIOS :
  - ➢ apporter la notion de lignes de défense en fonction de la criticité du bien à protéger
  - ➢ apporter à EBIOS l'atout de la démonstration de la défense par scénarios « enveloppe » ou par élément défaillant
  - ➢ affiner l'identification des risques résiduels
  - ➢ insérer les notions de barrières et de lignes de défense et de gravité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Conclusion

- ✓ L'étude conduite fait apparaître les points suivants :
  - ➢ un concept non développé en SSI même si le terme est souvent utilisé dans la littérature souvent pour regrouper des principes classiques ;
  - ➢ le concept est plus formalisé dans le monde industriel et constitue un référentiel partagé ;
  - ➢ le concept est utilisé pour la dynamique de réaction et pour la communication qu'il permet.
- ✓ Les apports du concept pour les maîtrises d'ouvrages :
  - ➢ un cadre permettant de mieux formaliser la notion de lignes de défense
  - ➢ un outil de communication en particulier au travers des niveaux de gravité d'un incident
  - ➢ une méthode intuitive permettant de rendre cohérent et d'unifier des mesures de protection par ailleurs connues
  - ➢ une méthode pour qualifier un système