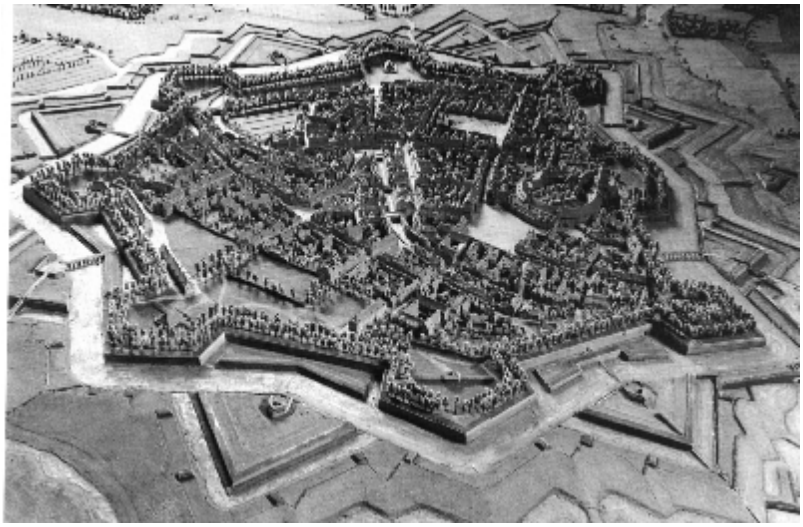
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

La défense en profondeur appliquée aux systèmes d'information

MÉMENTO



Version 1.0 – 4 novembre 2003

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Sommaire

Tables des figures

Introduction

1.1 Présentation de l'étude

La Direction Centrale de la sécurité des systèmes d'information (DCSSI) fait partie du Secrétariat Général de la Défense Nationale (SGDN). Elle a pour mission de contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information (SSI). Dans ce cadre, le bureau conseil de la DCSSI a mené une étude consacrée à la définition et la formalisation du concept de défense en profondeur appliquée au domaine de la sécurité des systèmes d'information. L'objet de l'étude est de permettre de dégager des conclusions pratiques et opérationnelles en matière d'architecture de SI et de gestion des risques.

1.2 Présentation du document

La démarche adoptée ayant conduit à l'élaboration de ce document est un déroulement selon 3 phases successives mais acceptant des recouvrements importants :

- la première phase a eu pour but d'étudier le concept de la défense en profondeur à partir :
  - d'entretiens avec des acteurs du monde industriel, car c'est dans celui-ci que ce concept est formalisé et autour duquel un effort de communication est important ;
  - de recherches bibliographiques sur le sujet ;
- la deuxième phase a eu pour objectif d'approfondir le concept et d'étudier son application au cas de la sécurité des systèmes d'information ;
- la troisième phase a eu pour objectif d'étudier la mise en œuvre du concept de défense en profondeur dans le cadre de la sécurité des systèmes d'information et en particulier sur le plan de la gestion des risques ; cette phase s'est appuyée sur un exemple.

Les différentes phases ont donc toutes comme idée la maîtrise des risques et en corollaire, comment les évaluer. Ce document reprend les livrables de chaque phase de l'étude pour en réaliser un résumé.

1.3 Plan du document

Ce document comprend trois parties principales qui sont le reflet de la démarche :

- la première partie fondée sur la recherche bibliographique et les entretiens menés dans le monde industriel et militaire essaye de déterminer les grands principes de la défense en profondeur ;
- la seconde expose la méthode issue des principes définis précédemment et applicable à la sécurité des systèmes d'information ;
- la troisième illustre la méthode à partir d'un cas concret ayant permis de mettre en évidence les modalités d'évaluation.

Une conclusion reprend les réflexions effectuées dans le cadre de cette étude pour en dégager les apports et orienter les travaux ultérieurs.

1.4 Bibliographie

Le tableau ci-dessous indique les documents les plus importants traités dans le cadre de cette étude. Lorsqu'une référence est citée dans ce document, le numéro correspondant est mis entre crochets (la numérotation de l'ensemble de la documentation de l'étude a été conservée).

N°	*Titre*
3	Security Architecture, Layered Insecurity
4	La défense en profondeur (Jacques VALANCOGNE de la RATP)
7	Defense in Depth
13	Small Business Guide to Network Security
17	Clefs CEA n°45 encadré D : les 3 barrières, illustration du concept de "défense en profondeur"
31	Defense-in-depth revisited: qualitive risk analysis methodology for complex network-centric operations
32	Chapter 2 Defense in Depth
33	Defense in Depth: Security for Network-Centric Warfare
43	Analyse des risques et prévention des accidents majeurs (DRA-007)
50	Annexe 8 : méthodologie d'analyse des conséquences potentielles (PROJET)
52	Evaluation quantitative de sécurité
53	Defense in Depth Strategy
55	Defense-in-Depth Overview (17/08/1998)

Tableau 1 : index bibliographique simplifié

1.5 Sigles et abréviations

Les sigles et abréviations utilisés dans ce document sont indiqués dans le tableau suivant.

Terme	*Signification*
AIEA	Agence Internationale de l'Energie Atomique
CDES	Commandement de la Doctrine et de l'Enseignement militaire Supérieur
DoD	Department of Defense (Département de la Défense des Etats-Unis)
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System (système de détection d'intrusion)
IIS	Internet Information Services (serveur internet Microsoft)
INERIS	Institut National de l'Environnement Industriel et des Risques
INSAG	International Nuclear Safety Advisor Group
IPSN	Institut de Protection et de Sûreté Nucléaire
SI	Système d'Information
SFEN	Société Française d'Energie Nucléaire
SSI	Sécurité des Systèmes d'Information

Tableau 2 : sigles et abréviations

2 Analyse du concept

2.1 Concepts au travers de la bibliographie

2.1.1 Étude du domaine militaire

Le concept de défense en profondeur semble prendre ses lettres de noblesse avec Vauban. L'apparition de boulets métalliques au XV^{ème} siècle capable de détruire les fortifications verticales entraîne la construction de fortifications beaucoup plus basses qui utilisent la profondeur du terrain. Les concepts sous-jacents sont les suivants :

- les biens à protéger sont **entourés** de plusieurs lignes de défense ;
- chaque ligne de défense participe à la **défense globale** ;
- chaque ligne de défense à un **rôle** à jouer : affaiblir l'attaque, la gêner, la retarder (échange de terrain contre du temps par exemple) ;
- chaque ligne de défense est **autonome** (la perte de la ligne précédente est prévue pour éviter un effet château de cartes) : la perte d'une ligne de défense affaiblit la suivante mais celle-ci dispose de ses propres moyens de défense face aux différentes attaques (chaque processus d'attaque possible entraîne une défense correspondante) ;
- Tous les moyens sont mis en œuvre pour renforcer la défense des différentes lignes :
  - utilisation du terrain (la fortification est un aménagement du terrain) ;
  - cloisonnement pour limiter les effets d'une percée et les tirs par ricochet ;
  - renseignement pour éviter la surprise.

Actuellement, le concept de défense en profondeur n'est plus à l'ordre du jour, la défensive n'étant que la résultante d'une position d'infériorité qui sera utilisée dans le but de reprendre l'initiative. Deux principes ont donc pris une très grande importance :

- le renseignement, qui permet de valider ou infirmer les hypothèses faites sur les actions ennemies, détecter son intention, etc. ;
- le mouvement (aspect dynamique de la défense).

Les grands principes de la défense en profondeurs sont les suivants :

- le **renseignement** est la première ligne de défense : depuis l'information sur les menaces effectives, la détection d'agissements souvent précurseurs d'attaques, jusqu'à toute détection non seulement d'attaques avérées et identifiées, mais encore de tout comportement « anormal » et donc suspect ;
- Il faut plusieurs lignes de défenses **coordonnées et ordonnées** par capacité de défense ;
- la perte d'une ligne de défense doit **affaiblir l'attaque** (au moins indirectement en recueillant un maximum d'information sur son ou ses origines, sa nature, sur les prochaines étapes possibles ou probables), ne pas entraîner la perte des autres lignes de défense mais au contraire permettre de les **renforcer** ;
- une ligne de défense doit comporter les parades (mêmes si cela se limite à détection d'anomalies et traçage dans le cas d'attaques de type non identifiable) à toutes les attaques possibles (**complétude** d'une ligne en elle-même) ;
- la défense n'exclue pas des actions offensives.

2.1.2Étude du domaine industriel

2.1.2.1 Nucléaire

Le concept de la défense en profondeur appliqué dans le cadre de la sûreté nucléaire, est issu des travaux consécutifs à l'accident de Three Miles Island du jeudi 29 mars 1979 où le cœur du réacteur, insuffisamment refroidi, fond partiellement. Elle est définie comme une défense comprenant trois barrières successives indépendantes qui ramènent à un niveau extrêmement faible la probabilité qu'un accident puisse avoir des répercussions à l'extérieur de la centrale. L'idée est que chaque dispositif de sécurité doit a priori être considéré comme vulnérable et doit donc être protégé par un autre dispositif.
L'EDF identifie également trois lignes de défense de natures différentes :

- La pertinence de la conception (en particulier la mise en œuvre de la redondance et de la diversification) ;
- La détection des défauts latents et des incidents ;
- La limitation des conséquences ("mitigation").

La défense en profondeur est associée à une gestion de risques dont les 8 niveaux normalisés sont présentés ci-dessous.

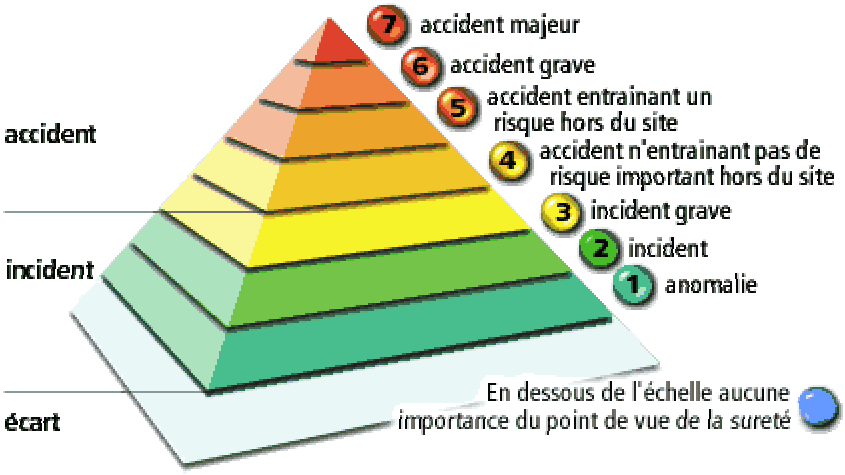


Figure 1 : échelle INES

Les trois barrières (la gaine du combustible, la cuve en acier du réacteur épaisse de 20 centimètres, l'enceinte de confinement (épaisse de 90 centimètres) qui entoure le réacteur[1] sont montrées dans le schéma ci-après.

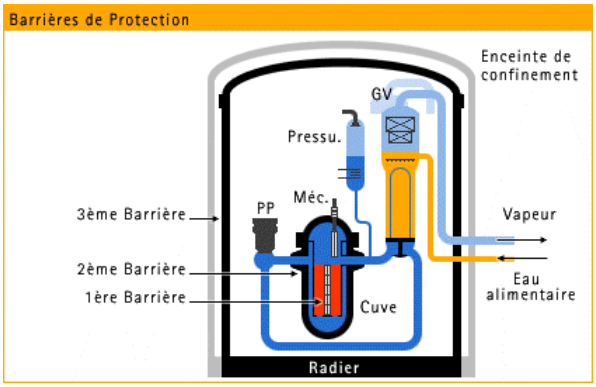


Figure 2 : les trois barrières

[1] Cette enceinte étant elle-même doublée dans les réacteurs modernes.

2.1.2.2 RATP

Les principes de défense en profondeur mis en œuvre dans le nucléaire se retrouve dans beaucoup de complexes industriels présentant des risques majeurs. Tout comme le nucléaire, le risque vient le plus souvent de l'intérieur et les différentes barrières ont pour objectif le confinement. Dans [4], J. Valancogne introduit une caractérisation des barrières :

- les barrières peuvent être soit technologiques, soit procédurales soit humaines. Elles peuvent être également mixtes, c'est-à-dire combiner ces différents attributs ;
- les barrières sont soit statiques soit dynamiques (une enceinte de confinement est une barrière statique alors qu'un automatisme chargé d'ouvrir une vanne est une barrière dynamique) ; Les barrières dynamiques (s'ouvrent et se ferment) peuvent être :
  - technologiques, humaines ou mixtes,
  - inhiber l'agression au moment où elle se manifeste (elle se ferme) ou au contraire s'ouvrir au flux si celui-ci n'est pas agressif (elle s'ouvre),
  - agir sur des échelles de temps différentes,
  - être en réussite ou en échec,
  - utiliser différents principes de réalisation (intrinsèque, probabiliste) ;
- elles peuvent agir soit sur l'élément agresseur, soit sur le flux, soit sur l'élément à protéger.

L'efficacité des barrières ne dépend pas uniquement de leur conception ; les aspects maintenance et évolution dans le temps sont également très importants. On peut associer à chaque barrière un arbre de défaillance. L'exemple de la catastrophe de Bhôpal, montre l'échec successif des trois barrières prévues pour éviter l'accident, principalement du fait de défauts de procédure et de maintenance. J. Valancogne insiste également sur l'importance du retour d'expérience et en particulier sur l'analyse des incidents (on retrouve ces éléments dans le nucléaire). De plus, le système n'étant pas figé, l'efficacité des défenses doit être réévaluée périodiquement.

2.1.2.3 Chimie

Un ouvrage particulièrement intéressant intitulé "Analyse des risques et prévention des accidents majeurs" (DRA-007) [43] a été publié par l'INERIS (Institut national de l'Environnement Industriel et des Risques). Il s'agit du rapport final (septembre 2002) du projet ASSURANCE dont l'objectif était de réaliser une analyse comparée des méthodes d'analyse des risques et approches sécurité en Europe au travers de l'étude d'une installation chimique réelle prise en référence. La démarche globale comprend les phases suivantes :

- détermination des risques ;
- hiérarchisation des risques :
  - classes de gravité en fonction des effets (létaux, irréversibles) ;
  - fréquence/probabilité en fonction du nombre de barrières ;
  - matrice d'acceptabilité des risques (en fonction de gravité et fréquence) : zones autorisées, acceptables et critiques ;
- analyse qualitative, les méthodes utilisées se répartissent en trois catégories :
  - les méthodes d'analyse inductives (la majorité : HAZSCAN, SWIFT, HAZOP, APR) sont fondées sur une analyse descendante de la séquence accidentelle (des causes vers les conséquences) ;

- les méthodes d'analyse déductives (arbre de défaillance) s'appuient sur une analyse ascendante de la séquence accidentelle (des conséquences vers les causes) ;
- les méthodes fondées sur l'identification systématique des causes de rejets, construites sur la base du jugement d'expert et du retour d'expérience (guide national ou grille d'audit).

- analyse quantitative, les méthodes utilisées se répartissent en deux catégories faisant l'objet du schéma ci-dessous :
  - approche probabiliste ;
  - approche déterministe.

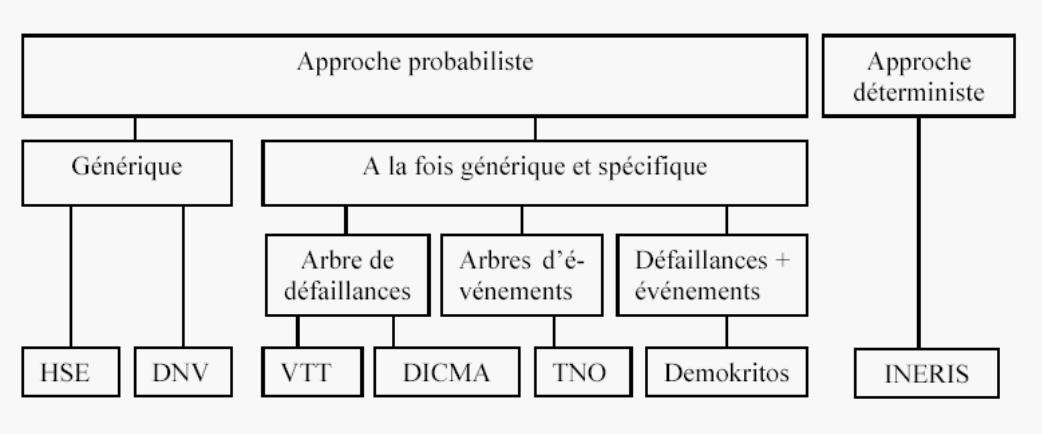


Figure 3 : les approches méthodologiques [43]

Suite à une analyse comparée entre les approches déterministe et probabiliste du risque, aucune des deux n'est parfaitement adaptée pour construire une politique cohérente et transparente de la gestion. Une solution alternative proposée serait alors de s'appuyer sur le concept des barrières de défense et de la défense en profondeur, qui est le principe fondateur de la sécurité, dans les installations nucléaires ou industrielles en France. De l'avis de l'INERIS, l'approche par barrières de défense permet plus de transparence dans la présentation de la gestion des risques, et donc une communication mieux perçue par le public et les associations.

2.1.3 Étude du domaine SSI

On distingue trois types de documents:

- des documents dans lesquels il ne s'agit d'une simple référence au bon sens : la défense ne doit pas se limiter à la périphérie ou reposer sur un moyen unique ;
- des documents, principalement aux Etats-Unis à partir de 1998, traitant de la sécurité des systèmes d'information du ministère de la défense en particulier et qui utilisent ce terme ;
- des documents qui sont plus méthodologiques ont été détaillés dans le document de la phase 2 :
  - [13] se voulant être une méthode simplifiée pour organisme de petite taille ;
  - [31] se rapprochant plus d'une analyse de risques qualitative ;
  - [3], prônant la défense en profondeur par un contre-exemple ;
  - [7], d'origine NSA à l'origine des concepts mis en œuvre par le DoD.

2.1.4 Analyse des contextes

Dans un premier temps il est nécessaire de prendre en compte les différences de contexte entre les trois domaines étudiés. Les points suivants paraissent intéressants :

- le facteur surprise :
  - dans le domaine militaire, il est systématiquement recherché et fait partie de la manœuvre ;
  - dans le domaine nucléaire, il est, sans doute, le facteur que l'on cherche à réduire au maximum même s'il ne doit pas être écarté ;
  - dans le domaine de la sécurité informatique, il est présent par le fait qu'il existera toujours de nouvelles formes d'attaques (actuellement la défense n'a pas l'initiative) ;

- le renseignement : il va en particulier permettre de diminuer l'incertitude sur les actions ennemies en confirmant ou infirmant les hypothèses et éviter les méfaits de la surprise ; le renseignement ne doit pas être dissocié de la planification ;

- la coopération entre les différentes lignes de défense :
  - dans le domaine militaire, il est systématiquement recherché la synergie entre les différents moyens : l'ajout d'un moyen supplémentaire doit procurer un avantage plus important que la simple somme des lignes de défense qui ne sont pas indépendantes ;
  - dans le domaine nucléaire, on insiste sur l'aspect d'indépendance vis-à-vis des menaces (les causes de défaillances) des différentes lignes de protection ;
  - dans la sécurité informatique il semble que l'ajout des dispositifs de protection est fortement lié à la présence de menaces, celles-ci étant prises de manière unitaire ;

- l'origine des menaces (interne/externe) :
  - la notion de défense rapprochée illustre bien ce principe : l'ennemi peut se trouver dans toute la profondeur du dispositif et par conséquent, quelque soit son rôle, chaque combattant doit assurer sa propre protection rapprochée ;
  - dans le milieu industriel, les menaces externes (terrorisme par exemple) sont prises en compte ; de même que les menaces internes (le processus industriel lui-même) ;
  - pour la sécurité informatique on retrouve le côté global de l'attaque qui provient de l'intérieur et de l'extérieur ; la profondeur du dispositif de protection doit donc être définies dans plusieurs dimensions ;

- pour qu'il y ait défense en profondeur il faut au minimum :
  - plusieurs lignes de défenses indépendantes dans le sens où chacune est capable de se défendre seule contre toutes les attaques (c'est-à-dire que la perte de la ligne précédente est prévue, il n'y a pas de présupposition que la ligne précédente existe) ; en toute rigueur il conviendrait de parler de lignes de défense autonomes ou complètes c'est-à-dire aptes à répondre à toutes les menaces ; en effet, l'un des principes de la doctrine militaire veut qu'en plus, les lignes participent à la défense globale qui présente alors une force de défense supérieure à la somme défense de

chaque ligne (ce point n'étant pas repris comme principe dans le milieu industriel qui s'attache plus à l'indépendance des barrières) ;

- coopération entre les lignes de défenses sinon le concept est ramené uniquement à de simples barrières successives dont la résistance ne dépend pas de la précédente (on peut alors les attaquer successivement) ;
- la perte d'une ligne doit permettre de renforcer la défense et non l'affaiblir (ce point étant un corollaire du précédent mais laissé ici pour apporter l'aspect dynamique de la défense).

Le schéma ci-après synthétise les relations entre les différentes approches recensées dans la bibliographie et illustre la convergence entre la sécurité des systèmes d'information et la gestion du risque industriel.

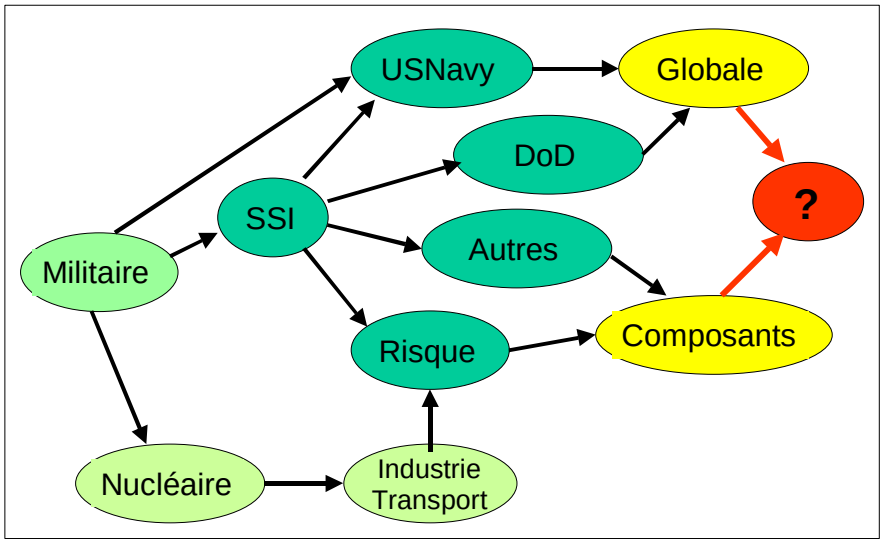


Figure 4 : approches de la défense en profondeur appliquée à la SSI

L'origine du concept de défense en profondeur est militaire. Ce mot est utilisé par la suite dans le domaine nucléaire qui en fait une méthode. Le concept est repris ensuite dans le cadre plus général de l'industrie (chimie) et des transports (RATP). Dans le milieu industriel, la défense en profondeur permet de compléter l'analyse de risques probabiliste par un aspect déterministe et une modélisation au niveau des composants. Le concept est ensuite repris au niveau de la sécurité des systèmes d'information aux Etats-Unis principalement mais sans le développer réellement, car il semble regrouper différentes notions qui tournent autour du mot profondeur dans le sens de plusieurs moyens redondants ou complémentaires. Toutefois deux approches semblent exister, la première insistant sur l'aspect global de la défense et l'autre plus orientée composants. C'est dans cette dernière approche que la référence à l'analyse de risque est plus explicite.

2.2 Apports des entretiens

De l'entretien mené avec des personnels militaires il ressort l'importance :

- du facteur renseignement, qui avait déjà été signalé, mais qu'il faut encore renforcer ;
- de l'aspect dynamique et de la planification ;
- des notions de responsabilité par niveaux.

Ces trois points doivent se traduire, dans le cadre de la défense en profondeur des systèmes d'information par la prise en compte des principes suivants :

- lors de la mise en place d'une "barrière", il faut prévoir en même temps :
  - le point de contrôle de son bon fonctionnement ou de sa chute (fonction renseignement) ;
  - les informations nécessaires à collecter pour savoir qu'un attaquant va la prendre pour cible ;
- lors de l'élaboration de la politique globale il faut prévoir la chute d'une barrière et donc :
  - prévoir des parades dynamiques ;
  - planifier les actions possibles en fonction des différents cas ;
- la sécurité du système d'information doit être la préoccupation de tous les personnels et non des seuls spécialistes ; des responsables doivent être nommés, à chaque niveau :
  - au niveau individuel (la sûreté immédiate) : charte, un manuel de procédure, etc. ;
  - au niveau de chaque cellule de l'organisation (la sûreté rapprochée) : dossier de sécurité adapté avec des procédures et un ou plusieurs plans de secours de niveau élémentaire ;
  - au niveau de l'organisme (la sûreté éloignée), les plans de secours vont avoir une portée plus générique de type multiservices, sites de secours, etc.

Le concept de la défense en profondeur doit être vu, dans le milieu industriel, comme un aboutissement logique de la maîtrise des risques :

- une fois l'objectif de sécurité défini (éviter une dissipation en dehors du site, un accident, etc.), une analyse du risque est menée selon des méthodes connues, la défense en profondeur combine donc à la fois l'approche déterministe et probabiliste ; ces deux approches complémentaires permettent de prévoir et mettre en place les barrières (approche déterministe au moment de la conception) puis d'évaluer la probabilité de défaillance des barrières (approche probabiliste) ;
- ensuite, on peut graduer les différents incidents dans une échelle globale qui a des avantages pédagogiques et médiatiques importants :
  - échelle de valeurs communes,
  - permet de présenter la défense selon un schéma compréhensible pour tous,
  - permet de déterminer facilement la gravité d'un incident qui est fonction de la barrière franchie ;
- enfin, chaque franchissement de barrière donne lieu à des mesures préventives et correctives et ce, en prévoyant jusqu'à la phase ultime lorsque le fait redouté arrive.

2.3 Conclusion de la première phase

Selon les critères définis pour la défense en profondeur, il n'a pas été trouvé de solution complète exposée dans le cadre de la sécurité des systèmes d'information. En contrepartie, les principes issus des domaines militaire et industriel apportent des idées intéressantes. En effet, le milieu militaire est proche de la sécurité informatique en ce qui concerne les aspects attaque/défense et le milieu industriel apporte le côté global, systématique et quantitatif et donc une rigueur mesurée qui manque dans le domaine informatique.
D'ors et déjà, il apparaît :

- que le terme de défense en profondeur, tel qu'il apparaît actuellement dans le cadre de la sécurité informatique ne représente pas une révolution par rapport aux principes appliqués actuellement, bien que certains auteurs fassent un effort de méthodologie sur le sujet ;
- que l'enrichissement des principes actuels de la sécurité informatique par des apports tirés de la méthode de défense en profondeur appliquée dans le milieu industriel et dans le domaine militaire devrait permettre de définir une réelle méthode de défense en profondeur dans laquelle il serait plus question de défense que de sécurité.

3 La méthode de défense en profondeur

3.1 Définition du concept

3.1.1 Appréciations générales du concept

Le principe le plus universel du concept de défense en profondeur et qui se retrouve dans les trois domaines, militaire, industriel et sécurité des systèmes d'information, est celui de plusieurs barrières indépendantes.

Les autres principes sont ensuite plus ou moins bien développés selon les cas. En outre, si dans le milieu industriel le concept est toujours le même, il faut reconnaître que dans la sécurité des systèmes d'informations, ce n'est pas le cas.

Il apparaît toutefois, que le concept de barrière est i) uniquement lié à la composante protectrice (contingentement, cloisonnement) et ignore donc d'autres dimensions essentielles ii) trop dépendant de la menace et donc délicat à manipuler au niveau de la sécurité des systèmes d'information lorsqu'on s'adresse à des décideurs ou des utilisateurs, principalement en raison de leur caractère technique et multiple.

En revanche, la notion de ligne de défense paraît être plus riche et plus parlante, même si cette notion est très arbitraire.

> Dans le cas, par exemple, d'un poste de travail protégé par un FireWall et un antivirus contre les accès non autorisés provenant de l'Internet, l'antivirus constitue la seconde barrière face à une tentative de déposer un code malicieux par intrusion mais la première si le vecteur utilisé est un courrier électronique, celui-ci étant autorisé par le FireWall. En effet, dans le cadre de la sécurité informatique, les moyens de protection (ici en l'occurrence le FireWall) sont plus un filtre que de véritables barrières comme dans le cas du nucléaire.

En effet, il n'est pas possible d'établir un lien direct entre barrière, ligne de défense et niveau de gravité en raison du caractère multiformes et multi-menaces de la défense. En contrepartie, la notion de ligne de défense permet de regrouper des barrières pour un aspect "communication" et de les corréler avec les niveaux de gravité[2]. Une ligne de défense correspond alors à une transition entre deux niveaux de gravité et implique une réaction planifiée correspondante.

La démarche proposée va donc conduire à déterminer les barrières[3] à mettre en place en fonction des menaces et des biens à protéger, puis à déterminer le niveau de gravité des incidents de sécurité provoqués par le franchissement des barrières afin de les regrouper par niveau de gravité et ainsi faire apparaître les lignes de défense. Celles-ci participent à l'effort de communication vers les décideurs et les utilisateurs mais ne remplacent pas l'étude des

[2] Les niveaux de gravité proposés sont indiqués plus avant dans le chapitre.

[3] Le terme de barrière (Cf. définition faite plus avant dans le chapitre) est pris ici comme synonyme de mesure de sécurité (humaine, procédurale, technologique) en reprenant la définition générique de ce terme proposée par M. Valancogne afin de conserver au terme ligne de défense un sens plus global et "communiquant". Nous écartons donc par là même le sens donné à ces deux termes par le CEA.

barrières pour les spécialistes de la sécurité. Cette démarche est présentée sur la figure suivante.

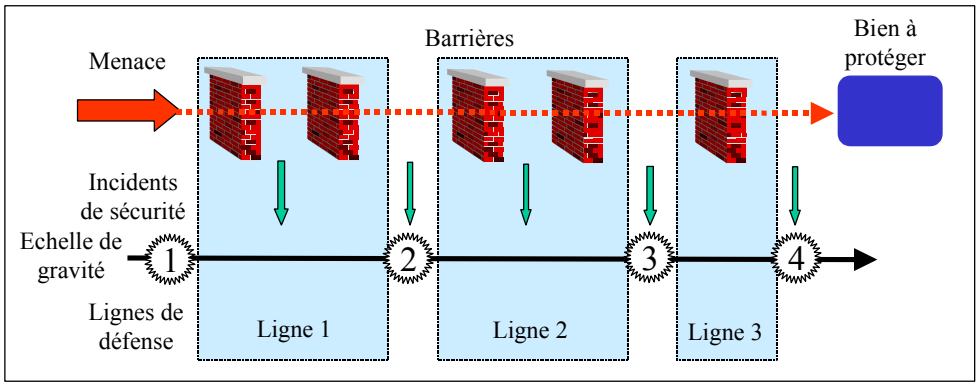


Figure 5 : démarche de mise en évidence des lignes de défense

La démarche doit combiner de manière itérative l'approche déductive (par les ressources) puis inductive (par les menaces). Elle arrête la conception lorsqu'il est possible de valider l'architecture et les moyens de protection et de déterminer les risques résiduels (qualification du système étudié).

Il est à noter que les barrières sont associées à des menaces (ce qui impose une approche inductive) mais que la gravité des incidents de sécurité dépend des ressources (ce qui impose une analyse de risque et une approche déductive). Les deux approches (inductive et déductive) se complètent donc l'une l'autre et sont à réitérer jusqu'à obtenir un niveau de protection suffisant. Il devient alors possible de valider l'architecture et les moyens de protection mis en œuvre en correspondance avec les risques et de faire apparaître les risques résiduels (qualification du système).

En outre, une barrière (et donc une ligne de défense) peut couvrir plusieurs menaces et son franchissement provoque un incident dont la gravité dépend du nombre de lignes de défense restant à franchir et de la valeur des biens à protéger. Il existe donc une double représentation :

- l'une pour les décideurs et les utilisateurs, volontairement globale et simple (l'aspect ligne de défense et échelle de gravité présenté sur le schéma précédent) ;

Cette représentation est importante pour l'aspect **communication** de la méthode.

- l'autre plus fine, s'appuyant sur des modélisations particulières des processus critiques par menaces principales et destinée aux spécialistes ; dans ce cas il sera sans doute intéressant de subdiviser les différents niveaux, subdivisions qui correspondraient alors à des variantes dans la planification (l'aspect scénario enchaînant barrières et incidents de gravité du schéma précédent).

Cette représentation est importante pour l'aspect **qualification** de la méthode (représentation schématique des différentes mesures de sécurité associées à une menace et protégeant un bien, élaborée lors de la construction des scénarii et qui permet : i) de déterminer les barrières à mettre en œuvre à partir de l'analyse inductive et puis déductive itérative jusqu'à obtenir le niveau de protection nécessaire ii) d'apprécier la gravité d'un événement de sécurité en fonction de la criticité du bien et du nombre de lignes restantes.

La modélisation particulière effectuée pour les biens critiques et les menaces principales permet de faire le lien direct et par conséquent de détecter les "trous de sécurité" plus facilement et par conséquent d'autoriser une évaluation.

3.1.2 Définitions

L'analyse des différents principes et du concept de défense en profondeur permet de proposer les définitions suivantes :

*La **gravité** d'un événement de sécurité mesure l'impact réel de l'événement en fonction de la criticité du bien (cas où un événement a une conséquence directe sur un bien) ou l'impact potentiel de cet événement sur le bien menacé en fonction du nombre de lignes de défense restantes et de la criticité de ce bien (cas ou l'événement n'a pas d'impact sur le bien mais sur ses moyens de défense).*

*Une échelle fixant les **niveaux de gravité** est proposée par la méthode afin de pouvoir comparer entre eux différents incidents de sécurité. Pour un incident de sécurité donné, il appartient aux responsables utilisateurs de déterminer le niveau de gravité correspondant qui s'apprécie en fonction de l'impact de cet incident sur le bien à protéger.*
*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.*

*Une **ligne de défense** est un ensemble de barrières, par scénario ou famille de scénarii, dont le franchissement provoque un incident dont la gravité dépend du nombre de barrières restantes à franchir par la ou les menaces pour atteindre le ou les biens protégés et de la valeur de ces biens (c'est-à-dire qu'à un incident de sécurité donné est associé un niveau de gravité qui indique la ligne de défense abstraite franchie). Toute ligne de défense pour être une ligne et pas seulement un ensemble de moyens de protection, doit être munie des dispositifs et moyens de détection/veille et de notification.*

*La **défense en profondeur** du système d'information est une défense globale et dynamique, coordonnant plusieurs lignes de défense couvrant toute la profondeur du système afin de permettre des actions de neutralisation des atteintes contre la sécurité, à moindre coût, grâce à une gestion des risques, un système de renseignement, une planification des réactions et l'enrichissement permanent grâce au retour d'expérience. Cette défense en profondeur a un double but : i) renforcer la protection du système d'information par une approche qualitative permettant de vérifier la complétude et la qualité du dispositif, ii) donner un moyen de communication fort permettant aux décideurs et aux utilisateurs de prendre conscience de la gravité des incidents de sécurité.*

Dans la sécurité des systèmes d'information, une barrière, un moyen ou dispositif, est associé à au moins une menace particulière et placé à un endroit bien défini (entre l'origine de l'agression et le bien à protéger). Elle peut protéger plusieurs biens mais pas obligatoirement de la même manière. Par conséquent, l'analyse des lignes de défense doit être effectuée pour chaque bien (ou ensemble de biens) et pour chaque menace donc pour chaque type d'incident de sécurité.
Cette analyse est faite avec une granularité qui dépend de l'importance du risque considéré (fonction de la criticité du bien et/ou de la probabilité d'apparition de la menace), en

combinant l'approche inductive (par les menaces) puis déductive (par les ressources à protéger).

3.2 Étapes de la méthode

La méthode s'inspirant de la défense en profondeur appliquée à la sécurité des systèmes d'information comprend les étapes suivantes :

- détermination des biens à défendre et des risques (les objectifs de sécurité) ; c'est à partir des résultats de cette étape que sera construite la défense en profondeur ; les objectifs de sécurité permettent de classifier les impacts sur l'échelle de gravité, ce qui permettra ensuite de fixer les incidents de sécurité sur cette échelle et donc de communiquer à partir d'un tableau des incidents associé à une représentation schématique du système d'information et des lignes de défense ;
- élaboration de l'organisation et de l'architecture générale du système (la profondeur du dispositif) ; c'est dans cette étape qu'il faut définir les points de contrôle et d'évaluation ; elle doit être menée le plus en amont possible dans les projets et permet de mettre en évidence les barrières, la gravité des incidents de sécurité (en fonction du nombre de barrières résiduelles) et les lignes de défense ; la cohérence globale du système ainsi que les mesures complémentaires prises dans l'étape suivante doivent permettre d'obtenir un haut niveau de protection **démontrable** ;
- élaboration de la politique de défense qui comprend deux volets : le premier organise le renseignement et le second la défense réactive correspondante *(inter-réaction, planification)* ; cette étape définit la politique opérationnelle de la défense et met en évidence les points de contrôle ; cette politique de défense doit permettre l'observation du système, la remontée des événements de sécurité pour alimenter le tableau de bord et la prise de décisions sur les moyens de réaction à mettre en œuvre ; cette étape a un aspect opérationnel et dynamique alors que la précédente est plus statique ;
- évaluation de la défense permanente et périodique à partir des méthodes d'attaques et du retour d'expérience ; cette étape correspond à la partie contrôle et audit ;
- mise à jour de la défense à partir des résultats de l'évaluation et pour prendre en compte les évolutions ; cette étape correspond aux opérations de maintien en condition de sécurité.

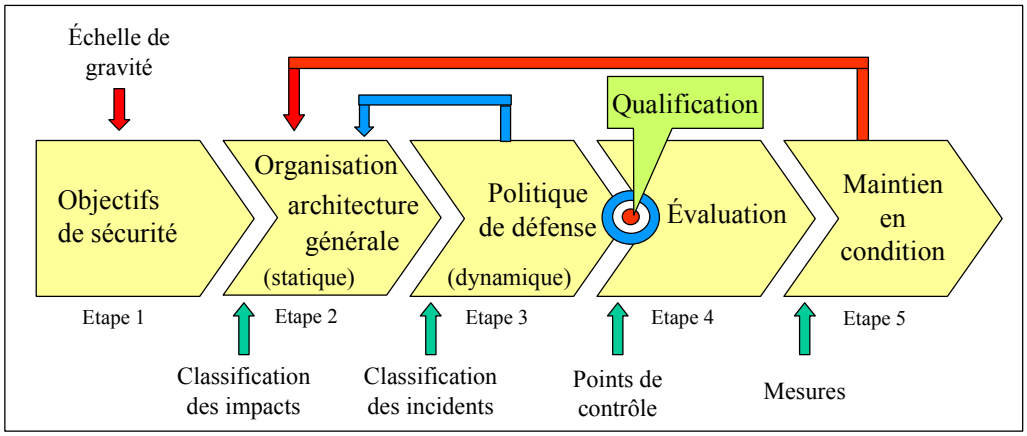


Figure 6 : les étapes de la méthode

3.2.1 Première étape : détermination des objectifs de sécurité

Cette première étape se compose donc des actions suivantes, somme toute classiques : détermination des biens à défendre et de leur criticité (l'analyse de risque qui permettra ensuite de quantifier la valeur de la défense : la fiabilité d'un équipement doit être pondérée par la valeur de la conséquence de sa perte pour graduer le niveau d'alerte).

A l'issue de cette étape préliminaire, les acteurs du modèle sont identifiés et les besoins de sécurité sont définis.

Une méthode de type EBIOS paraît particulièrement adapté pour réaliser cette étape préliminaire. Toutefois, il est nécessaire de bien déterminer, si possible sur une échelle de valeur au minimum relative, les critères qui seront utilisés pour l'évaluation.

L'échelle de gravité proposée pour classer les événements de sécurité en fonction de leur impact sur le système d'information est indiquée dans le tableau suivant. Elle est inspirée de l'échelle INES.
Toutefois, l'échelle INES distingue les incidents des accidents en fonction de l'impact hors site ou non de l'événement. Dans le cadre de la sécurité des systèmes d'information, cette distinction n'a pas de raison d'être. L'échelle proposée est donc fondée uniquement sur l'impact de l'événement.

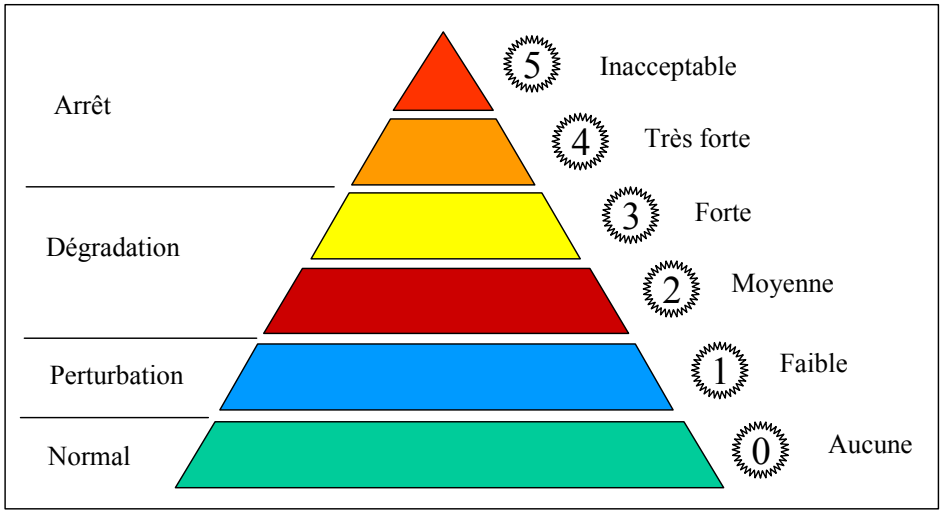


Figure 7 : : échelle de gravité SSI

Catégorie	Niveau	Gravité	Critère
Arrêt	5	Inacceptable	L'événement met en cause la survie de l'entreprise (le fait redouté est arrivé).
	4	Très forte	L'événement présente un risque très important et nécessite donc des mesures d'urgence immédiates.
Dégradation	3	Forte	L'événement n'entraîne pas de risque important mais une partie significative du système a été touchée.
	2	Moyenne	L'événement a une conséquences sur le fonctionnement normal et doit entraîner une réaction immédiate.
Perturbation	1	Faible	L'événement n'a pas de conséquences notables mais doit être traité pour rétablir un fonctionnement normal.
Fonctionnement normal	0	Aucune importance du point de vue de la sécurité	Fonctionnement normal.

Tableau 3 : échelle de gravité SSI.

Dans cette étape, il s'agit donc d'indiquer le niveau de gravité des principaux événements redoutés (on pourra prendre les facteurs de risque étudiés dans l'analyse de risque par exemple) pour les différents biens à protéger.
Il importe que l'analyse menée à cette étape soit le fruit de la combinaison et validation mutuelle d'une approche déductive (par les ressources) puis inductive (par les menaces) et que soit pris en compte le facteur humain. Les scénarii élaborés lors de cette étape seront modélisés dans l'étape suivante.

3.2.2 Deuxième étape : architecture générale du système

Cette étape vise à déterminer la profondeur du dispositif :

- découpage des zones en fonction des risques, des acteurs, des grandes fonctions de l'entreprise (l'urbanisation du système d'information) ; ce découpage est établi selon les principes d'indépendance des entités et de cloisonnement ;
- détermination des barrières (moyen technique, procédural et humain) ;
- classification des zones en fonction de leur sensibilité et détermination des règles de passage de l'une à l'autre (c'est dans cette étape qu'il convient de traiter le cas de la classification des informations et des mesures à prendre pour l'interconnexion de deux domaines de niveaux de sécurité différents) ;
- découpage des zones en domaines de confiance : introduction des cloisonnements organisationnels en général (la profondeur de l'organisation) ;
- répartition privé/commun dans chaque domaine et entre domaines.

Il paraît indispensable dans cette étape :

- d'établir un "tableau des mesures" prises afin de bien montrer les moyens de défense dans toute la profondeur ;
- de modéliser les systèmes critiques afin de les évaluer ;
- de fixer les incidents (franchissement d'une barrière) sur l'échelle de gravité globale en fonction de la classification des impacts définie précédemment, car elle permettra au niveau de la politique opérationnelle d'apporter la graduation des actions et de définir les lignes de défense (c'est dans cette étape que la transposition des barrières en lignes de défense est effectuée).

La modélisation est effectuée pour les biens critiques et les menaces principales seulement afin de minimiser le nombre de scénario. Elle est pratiquée en deux phases :

- l'une pour mettre en évidence un nombre de barrières en cohérence avec la gravité de l'événement redouté,
- l'autre pour valider le résultat par l'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.

Cette étape doit être menée normalement en amont des projets c'est-à-dire qu'une étude de sécurité doit être **intégrée** dans la méthode de gestion de projet. Dans la mesure où le système existe déjà, la méthode est la suivante :

- analyser la topologie du système d'information, tant technique que fonctionnelle ;
- identifier les barrières existantes ;
- modéliser les processus les plus importants (modélisation des données critiques et des principales menaces afin de mettre en évidence les barrières) ;
- évaluer l'architecture déjà en place pour déterminer les modifications à apporter afin qu'elle réponde aux critères (ajout de nouvelles barrières par exemple).

3.2.3Troisième étape : élaboration de la politique de défense

Cette étape est composée de trois sous-étapes :

- détermination de la défense globale et coordonnée :
  - détection (détermination des points de contrôle et de détection des attaques) ;
  - remontée de l'information ;
  - corrélation des événements ;
  - alerte ;

- planification :
  - détermination des reconfigurations possibles, avec un fonctionnement normal (dispositif de tolérance aux pannes avec des performances identiques) et avec un fonctionnement en mode dégradé (par exemple : fonctionnement en local uniquement, performances moindres, etc.) ;
  - plans de réaction (planification des actions possibles en fonction des événements redoutés, plan de continuité par exemple mais aussi reconfiguration réseau, mise en œuvre de moyens de secours, etc.).

- qualification (validation de l'organisation et de l'architecture) :
  - formelle : respect des principes de la défense en profondeur (globalité, indépendance, points de contrôle, etc.) et respect de la méthode telle qu'elle peut être formalisée au niveau de l'organisme ;
  - démonstrative au travers de l'étude des scénarii applicables.
  -

Les deux premières étapes ne sont pas séquentielles mais itératives jusqu'à obtenir le niveau de sécurité exigé par la criticité de la ressources à protéger, des menaces potentielles et des risques résiduels. La troisième étape permet de mettre en évidence les risques résiduels qui doivent être connus et acceptés.

La défense globale se décline selon les trois axes (humain, procédure, technologie) qui intègrent les lignes de défense déployées sur les zones définies à l'étape précédente. Chaque ligne dispose idéalement de trois fonctions de sécurité : protection, détection et réaction. La politique de défense doit déterminer pour les différents incidents de sécurité leur gravité afin de bénéficier de l'apport "pédagogique" de la méthode permettant une meilleure sensibilisation des personnels. Les niveaux de gravité des incidents seront déduits ensuite à partir du nombre de lignes de défense restantes.

La gravité d'un incident dépend plus des moyens de défense restants que de ceux qui ont été franchis. En effet, par exemple une attaque interne peut permettre de sauter plusieurs barrières qui seraient à franchir en cas d'attaque externe. Il est à noter que la règle veut :

- qu'il y ait au minimum 3 lignes de défense[4] ;
- que le nombre de lignes de défense doit être adapté au risque (probabilité d'occurrence et criticité du bien).
-

La défense doit être à la fois globale (tous les moyens participent au même objectif de sécurité) et coordonnée. Cette coordination concerne principalement les moyens de renseignement (permet de préciser la menace réelle par analyse de plusieurs informations concernant une attaque en cours) et de réaction (reconfiguration de moyens de défense à partir de la détection d'un autre moyen de défense, y compris des moyens de filtrage). Il est à noter que cette coordination concerne les barrières et non les lignes de défense.

La dynamique de la défense est apportée par la planification des réactions en cas d'atteinte à la sécurité. Les incidents et accidents doivent être classifiés selon l'échelle de gravité et déclencher obligatoirement une réaction qui est du niveau technique (réponse automatique), procédural (application de la procédure ou du plan correspondant) ou humaine (décision, initiative, etc.). Les plans de réactions doivent être gradués de la même manière que les atteintes à la sécurité pour renforcer les mesures en fonction du niveau de gravité. En effet, dans le cadre de la défense en profondeur, la prise en compte de plusieurs incidents en même temps doit être prévue.

Parmi les mesures non-techniques à prendre, celles visant à des actions en justice contre des tiers extérieurs sont à prévoir de même que celles prévues au règlement intérieur contre les personnels de l'entreprise (à la technique de fournir les éléments de preuves qui étayerons ces mesures).

Cette étape se termine par la qualification (validation de l'organisation et de l'architecture) du système qui résulte de deux approches :

- l'une **formelle** : respect des principes de la défense en profondeur (globalité, indépendance, points de contrôle, etc.) et respect de la méthode telle qu'elle peut être formalisée au niveau de l'organisme ; cette partie s'apparente donc à une démarche qualité ;
- l'autre **démonstrative** au travers de l'étude des scénarii applicables.

[4] De manière simpliste on considère que l'une des trois est affectée par l'incident ou l'agression initiateur de l'incident, l'une des deux autres est défaillante pour une raison fortuite et les conséquences sont limitées "à coup sûr" par la troisième.

Cette deuxième partie de la qualification, spécifique de la défense en profondeur, doit permettre de vérifier :

- l'exhaustivité des scénarii :
  - ceux-ci doivent normalement être réalisés pour les biens critiques et pour les menaces critiques ;
  - afin d'en diminuer leur nombre, il est possible de :
    - les regrouper par famille pour faire apparaître les similitudes,
    - déterminer des scénarii "enveloppes", c'est-à-dire des scénarii, qui souvent modélisent le pire cas redouté, à l'intérieur desquels les autres scénarii peuvent s'inscrire ;
- la cohérence entre le nombre de lignes de défense et la gravité des événement redoutés déterminée à la fin de la première étape ainsi que l'acceptation des risques résiduels en cas d'insuffisance.

3.2.4 Quatrième étape : évaluation permanente et périodique

3.2.4.1 Contenu de l'étape

Cette étape a pour objet d'évaluer la défense de manière systématique :

- étude statique des composants ;
- dynamique sur incident (retour d'expérience) ;
- tableau de bord ;
- audit périodique ;
- rétroaction (Cf. ci-après).

Cette étape est étroitement liée à la suivante car elle participe au même but, actualiser la défense et la renforcer en prenant deux critères essentiels tirés de l'exemple de la RATP pour les cas non quantifiables en terme de coût/gain :

- ne pas régresser ;
- améliorer si le coût en vaut la peine.

Les résultats de cette étape doivent permettre de présenter aux décideurs les mesures prises pour satisfaire aux besoins de sécurité définis à l'étape 1 et ainsi démontrer que les objectifs sont bien atteints.

Un effort de communication est à effectuer dans cette étape pour regrouper les scénarii par famille et mettre en évidence les principales lignes de défense ainsi que les mesures planifiées de réaction prévues.

3.2.4.2 Objectifs et méthodes d'évaluation

La méthode d'évaluation doit être cohérente avec la méthode globale de défense en profondeur telle qu'elle a été construite et en particulier s'appuyer sur les différents résultats produits pendant les différentes étapes.
En outre, l'évaluation doit être à la fois périodique (mise en place initiale et révision périodique proprement dite) et permanente (exploitation du retour d'expérience et de la veille technologique). Cette méthode est schématisée dans la figure ci-dessous et explicitée ci-après.

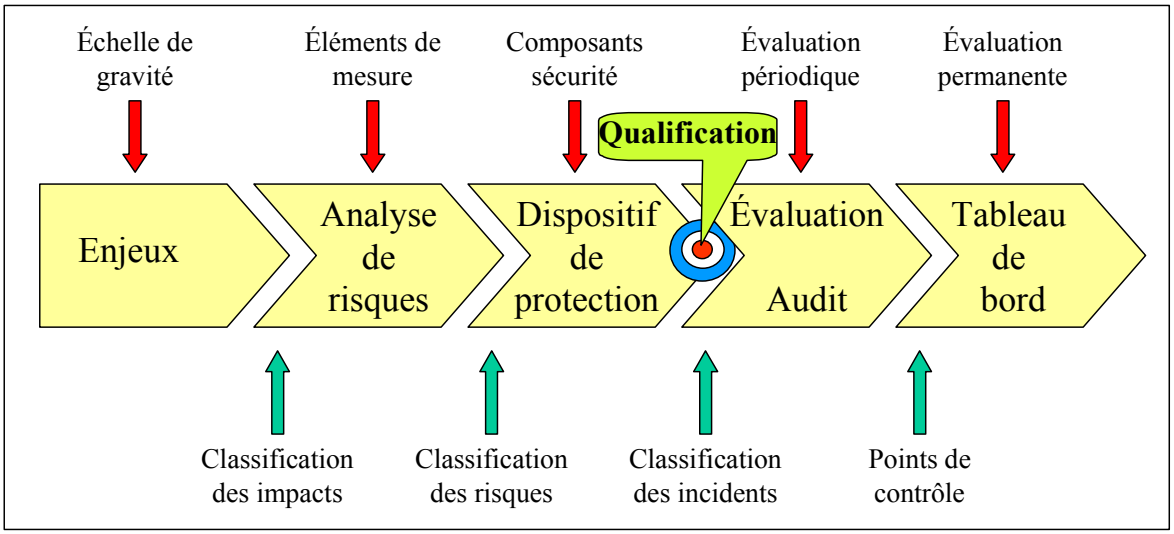


Figure 8 : principes d'une évaluation

La première étape, détermination des objectifs de sécurité, permet d'une part de classer les impacts potentiels sur l'échelle de gravité en fonction des enjeux et d'autre part de déterminer les éléments de mesure pour classifier les risques.

La seconde étape, architecture du système, a comme résultat un classement des incidents de sécurité en fonction des composants défaillants.

La troisième étape, élaboration de la politique de défense, a mis en évidence les points de contrôle qui seront utilisés pour l'évaluation permanente du dispositif au cours de la quatrième étape d'évaluation permanente et périodique.

La méthode s'appuie donc sur :

- une méthode d'analyse de risques de la sécurité des systèmes d'information complétée par la hiérarchisation des risques par composants principaux et par fonctions de sécurité sur l'échelle de gravité, définie précédemment, qui permet de classer les incidents de sécurité ;
- une modélisation de la défense en profondeur appliquée aux risques principaux et l'analyse des scénarii les plus importants (scénarii "enveloppe" en particulier) ou les plus probables ; ces scénarii sont itératifs ; ils permettent de déterminer les barrières et d'évaluer la défense en pratiquant la méthode du composant défaillant jusqu'à obtenir la "démonstration" de la robustesse de la défense ;
- une classification des incidents de sécurité sur l'échelle de gravité précédente effectuée en fonction des risques définis ; les points de contrôle du bon fonctionnement ainsi que ceux permettant de détecter les attaques éventuelles sont mis en évidence ; ils permettront de procéder à l'évaluation permanente et périodique ;
- les évaluations menées d'une part par les méthodes d'audit habituelles et d'autre part par l'évaluation des défenses au travers des scénarii et des incidents de sécurité (recherche des conséquences potentielles) ;
- les différentes études permettant de démontrer le niveau de sécurité atteint et de communiquer sur le sujet pour mettre en place la défense en profondeur et sensibiliser les personnels aux incidents de sécurité (aspect communication renforcé par la présence d'un tableau de bord de sécurité mettant en évidence les incidents sur l'échelle de gravité).

La méthode d'évaluation de défense en profondeur utilise donc deux méthodes d'analyse qui sont :

- l'analyse par scénario "enveloppe" : cette analyse consiste à établir un scénario couvrant le risque maximum (la destruction du site principal) et de montrer que les autres scénarii (impossibilité de rentrer dans le site principal par exemple) sont inclus dans le cas "enveloppe" et donc que la solution retenue les couvre ;
- l'analyse par "composant défaillant" (Cf. définition précédente).

En conséquence, la méthode complète l'analyse qualitative globale classique par une analyse quantitative de type déterministe dans les cas particuliers des scénarii de risques importants en utilisant la notion de scénario enveloppe et de composant défaillant. Cette méthode est bien adaptée au principe de "démonstration" de la sécurité qui est la règle dans le cas de la sûreté nucléaire et qu'il convient de promouvoir.

3.2.5 Cinquième étape : organiser le maintien en condition (MCS)

Cette étape a pour but de prendre en compte les évolutions et les résultats de l'évaluation :

- le système lui-même ;
- les risques ;
- la vulnérabilité ;
- une nouvelle méthode ;
- la veille technologique ;
- etc.

3.3 Les apports de la méthode

Par rapport aux méthodes habituellement utilisées pour la sécurité des systèmes d'information ou proposées dans la bibliographie et se présentant comme issues de la méthode de défense en profondeur, la méthode proposée ci-dessus paraît apporter les améliorations suivantes issues de l'étude du concept dans le monde industriel et militaire :

- importance de **l'analyse quantitative** permettant d'évaluer le système dans le futur ;
- qualification à partir des **modélisations** particulières donnant une évaluation initiale ; en effet, des scénarii enveloppes paraissent bien mieux adaptés et plus réalisables que des analyses probabilistes ;
- **profondeur de l'organisation** s'appuyant sur une démonstration de la sûreté du dispositif à partir des scénarii et des lignes de défense ;
- évaluation selon une **échelle de gravité**, type échelle INES, apportant un aspect **communication** très fort ;
- aspect **global** de la défense ;
- importance du **renseignement** et de l'observation (points de contrôle) préservant la liberté d'action ;
- aspect **dynamique** de la défense intégrant le processus veille, alerte, réponse et la planification ;
- **évolutivité** de la défense par retour d'expériences (recherche des conséquences potentielles et non seulement des causes), celui-ci permettant de valider les scénarii, les mettre à jours, etc.

Il ne faut pas oublier non plus que le terme de **défense** (au lieu de sécurité) est porteur d'idées fortes car il apporte les notions de dynamique, d'initiative et de liberté d'action, de fonctionnement dégradé etc. et ne cantonne pas à mettre de la protection en place. Il parait toutefois intéressant de mener une réflexion sur la formalisation de la représentation, par exemple en se fondant sur la théorie des graphes, mais cette réflexion sort du cadre de cette étude (cf. à ce sujet l'analyse quantitative des risques proposée par [52]).

4 Application de la méthode proposée

Dans ce document seuls les points particuliers les plus significatifs de la méthode sont présentés, l'exemple complet étant disponible par ailleurs.

4.1 Présentation du cas concret

Le cas concret étudié est celui d'une petite entreprise spécialisée dans l'importation de produits étrangers et qui joue le rôle de grossiste vis-à-vis de revendeurs. Ces revendeurs sont identifiés avant toute transaction (contrôle de la solidité financière, détermination des conditions de vente et de paiement, etc.). Les marchandises sont stockées au plus près des points de dédouanement (port et aéroports) afin de minimiser les transports vers les revendeurs qui sont situés dans toute la France.
Sur le plan de la sécurité, le système de ventes (seul étudié ici) se compose des éléments suivants :

- le système de ventes proprement dit (matériel et logiciel et réseau intranet) ;
- l'interface avec les clients permettant de recevoir les commandes par e-mail Internet (système de communication comprenant un dispositif d'accès à Internet et un système de messagerie) ;
- l'interface avec les magasins (système de communication de type intranet étendu) ;
- l'interface avec la comptabilité (système d'interconnexion de deux intranets).

4.2 Déroulement de la méthode

La première étape permet de définir les besoins de sécurité du système global et de ses composantes par critère dont la synthèse est présentée dans le tableau ci-dessous.

Sous-système	Disponibilité	Intégrité	Confidentialité
Système de ventes proprement dit	Interruption < 1h	Non altération des données	Informations confidentielles
Réception des commandes	Interruption < 2h	Non altération des données	Confidentialité par chiffrement (utilisation Internet)
Communication avec les magasins	Interruption < 1h	Non altération des données	Confidentialité par chiffrement (utilisation Internet)
Communication avec la comptabilité	Interruption < 4h	Non altération des données	Informations confidentielles

Tableau 4 : besoins de sécurité par critères

La méthode devant apporter les moyens de l'évaluation, il paraît important à cette étape de l'étude de hiérarchiser les objectifs de sécurité. Cette hiérarchisation permet ensuite de graduer les incidents selon l'échelle de gravité proposée par la méthode. Pour cette hiérarchisation, il convient de prendre en compte les conséquences potentielles des incidents de sécurité.

L'analyse du tableau précédent montre qu'il existe une hiérarchisation implicite des biens à protéger qui sont dans l'ordre décroissant : le système de ventes proprement dit, le système de réception des commandes, le système de communication avec les magasins, le système de communication avec la comptabilité.

De même il existe une hiérarchisation des objectifs de sécurité : la disponibilité est primordiale, l'intégrité est jugée moins importante que la confidentialité. Le tableau ci-dessous présente donc un exemple de la hiérarchie des incidents potentiels telle qu'elle peut se dégager en utilisant l'échelle de gravité proposée par la méthode.

Gravité de l'événement redouté	Atteinte grave aux besoins de sécurité exprimés pour le critère			
	Disponibilité	**Intégrité**	**Confidentialité**	**Preuve et contrôle**
5 – Inacceptable	Système de ventes			
4 – Très forte	Réception des commandes		Système de ventes	
3 – Forte	Communication magasin	Système de ventes	Réception des commandes	Réception des commandes
2 - Moyenne	Communication comptabilité	Réception des commandes	Communication magasin	Système de ventes
1 - Faible		Communication magasin et comptabilité	Communication comptabilité	Communication magasin et comptabilité

Tableau 5 : hiérarchisation des événements redoutés

S'agissant dans ce document d'un exemple, la modélisation des chaînes de liaison ne concerne que les risques liés à la présence de communications avec les revendeurs utilisant le canal Internet, en considérant qu'il est prévu un moyen de cryptographie permettant d'authentifier le correspondant, de garantir l'intégrité des données et de préserver leur confidentialité ainsi qu'un système applicatif de contrôle des commandes.

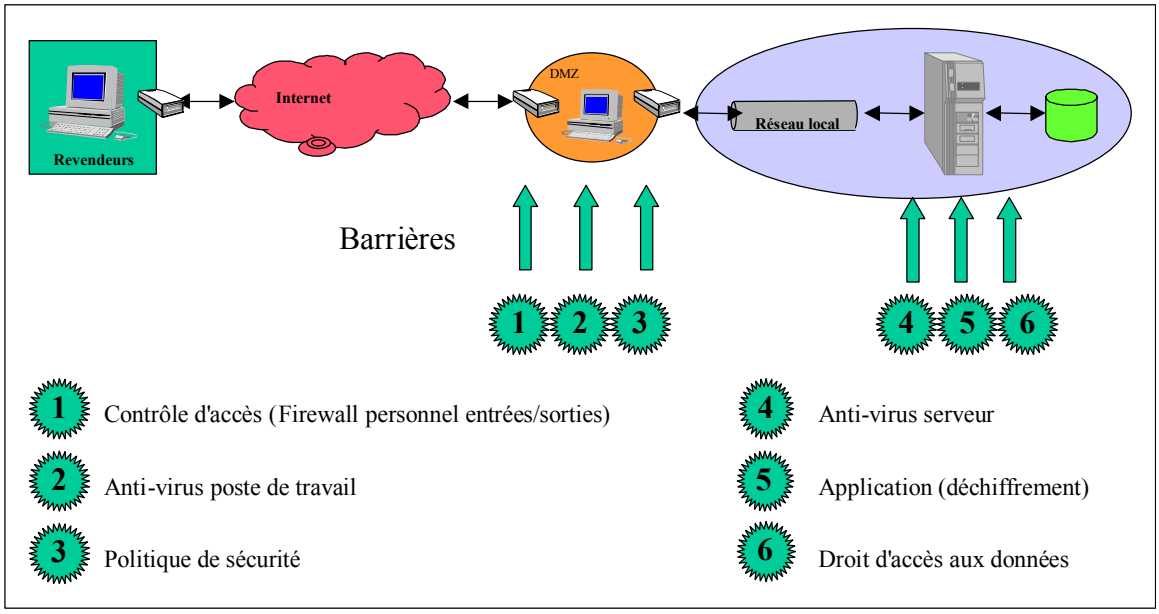


Figure 9 : modélisation de la chaîne de liaison "commandes"

Il est à noter que la méthode est itérative et peut être utilisée aussi bien pour déterminer les lignes de défense à mettre en place que pour valider les lignes de défense prévues. Cette double utilisation permet de capitaliser sur le retour d'expériences (quatrième étape).

Dans le cas ci-dessous, cette modélisation est effectuée en construisant les scénarii à risques et en mettant en évidence les lignes de défense. Pour cette construction :

- la **source de danger** est un tiers non identifié ;
- l'**événement initial** est soit un faux message, soit un accès non autorisé (comme on autorise les messages entrants, la première barrière est différente selon les cas) ;
- **l'événement redouté** est une atteinte à la sécurité du système d'information :
  - contre l'intégrité des données : acceptation d'une fausse commande ;
  - contre la disponibilité du SI : indisponibilité du serveur ;
  - contre la confidentialité des données : évasion d'information.

Le schéma ci-après synthétise les trois scénarii étudiés et explicités ci-après.

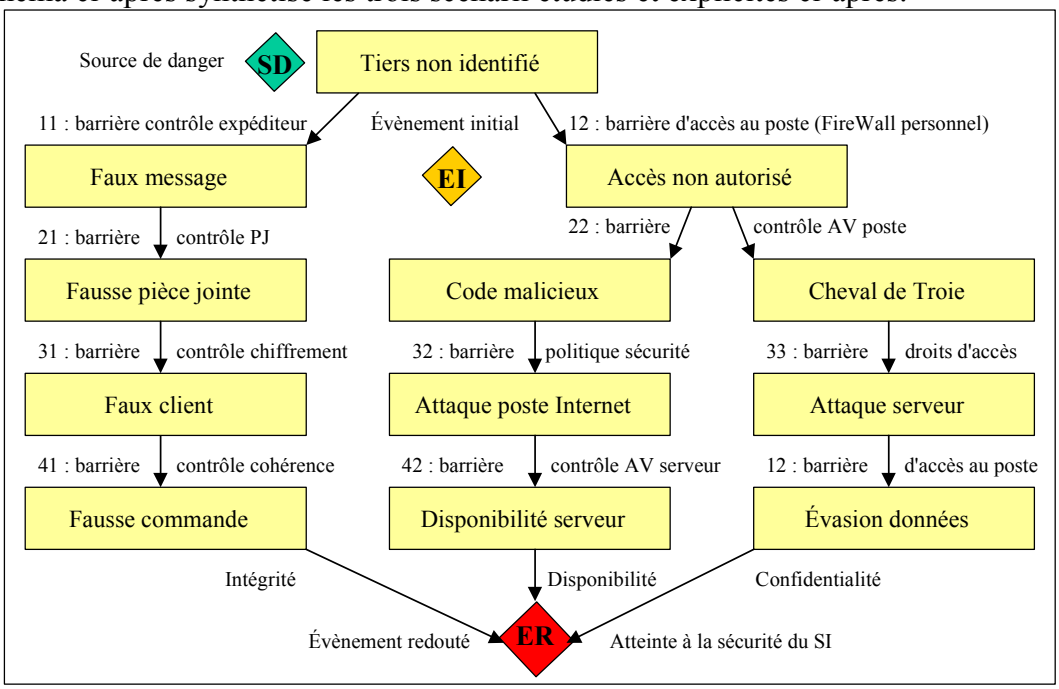


Figure 10 : scénarii à risque

Le premier scénario étudie le cas de la réception d'un message qui pourrait être pris pour un vrai message et donc porter atteinte à l'intégrité su système d'information. Ce message passe au travers du contrôle d'accès au poste car celui-ci accepte les messages entrant.

Le deuxième et le troisième scénario étudient les cas d'un accès non autorisé introduisant un code malicieux. Dans le deuxième scénario, il s'agit d'un virus destructeur qui risque de porter atteinte à la disponibilité du système d'information. Enfin, dans le troisième il s'agit d'un cheval de Troie qui essaye de faire sortir des informations.

L'analyse par composant défaillant dans le cadre du scénario 2 fait apparaître la nécessité de durcir le poste de travail :

- si l'on considère un code malicieux arrivé par messagerie et non détecté par l'antivirus, il ne reste que la politique de sécurité du poste (en effet, il est courant de mettre la même famille d'antivirus sur les postes de travail et sur le serveur) ;

- en cas de défaillance de la politique de sécurité, il n'existe plus aucune barrière avant l'événement redouté, ce qui est insuffisant.

La mise en évidence des barrières de sécurité permet de prévoir le niveau de gravité des incidents de sécurité. En effet, la hiérarchisation des risques fournit une échelle des conséquences potentielles (la gravité des événements redoutés) et l'analyse par composants détermine, pour un événement initial, le nombre de barrières restantes. Le tableau ci-après classe donc les trois types d'incident, objets des trois scénarii, sur l'échelle de gravité précédente.

Gravité	Code malicieux (Disponibilité)	Faux message (Intégrité)	Cheval de Troie (Confidentialité)
5 – Inacceptable	Serveur indisponible		
4 – Très forte	Poste Internet indisponible		Evasion de données
3 – Forte	Code malicieux sur poste Internet	Fausse commande	Détection d'une tentative d'accès au serveur
2 – Moyenne	Code malicieux détecté par antivirus du poste Internet	Détection fausse commande au niveau chiffrement	Cheval de Troie détecté par antivirus du poste Internet
1 – Faible	Tentative d'intrusion bloquée par le FireWall	Détection fausse PJ ou expéditeur inconnu	Tentative d'intrusion bloquée par le FireWall

Tableau 6 : hiérarchisation des incidents prévus

Les différentes lignes de défense mises en évidence par rapport au bien critique que constitue le serveur supportant le système des ventes par rapport à une menace extérieure sont indiquées dans le tableau suivant, ainsi que les mesures de sécurité prévues.

Ligne	Code malicieux (Disponibilité)	Faux message (Intégrité)	Cheval de Troie (Confidentialité)
1	▪ FireWall personnel	▪ Contrôle expéditeur ▪ Contrôle pièce jointe	▪ FireWall personnel
2	▪ Antivirus du poste	▪ Contrôle du chiffrement ▪ Contrôle de cohérence de la commande	▪ Antivirus du poste
3	▪ Politique de sécurité du poste		▪ FireWall personnel ▪ Contrôle d'accès serveur
4	▪ Antivirus du serveur		

Tableau 7 : Tableau des mesures de sécurité

5 Conclusions de l'étude

L'étude de la défense en profondeur dans le cadre de la sécurité des systèmes d'information fait apparaître :

- que le concept n'est pas développé actuellement dans le cadre de la SSI, même si ce terme est utilisé dans la littérature, principalement aux Etats-Unis à partir de 1998, pour regrouper différents principes largement diffusés ;
- que le concept mis en œuvre dans le milieu industriel est plus riche que les méthodes d'analyse de risques utilisées habituellement mais reste pragmatique et par là même est facilement transposable ;
- que le concept, avec sa dynamique et sa facilité de communication, est un enrichissement notable des méthodes habituelles avec lesquelles il est compatibles.

Des axes d'étude complémentaires paraissent intéressants :

- le développement d'un outillage de la méthode afin de modéliser les scénarii et de faire apparaître les lignes de défense en fonction des conséquences des incidents de sécurité ;
- la formalisation de la méthode et un travail de recensement des composants, moyens de contrôles, moyens de détection des attaques, etc. ;
- la réalisation d'ensembles de composants d'architectures types, dont la résistance est éprouvée, permettant de capitaliser sur les différentes études (par exemple pour les centrales nucléaires de même technologie) ; ces ensembles devraient être modulaires pour être réutilisables ;
- la réalisation d'études plus théoriques sur la détermination d'une probabilité de résistance des composants qui devrait être liée à une notion de certification ou à l'évaluation quantitative de la sécurité [52] au travers d'une modélisation des vulnérabilités (par exemple sous forme d'un graphe des privilèges transformé ensuite en réseau de Petri stochastique généralisé).

Ce document est un résumé de l'étude de la défense en profondeur appliquée à la sécurité des systèmes d'information qui fait l'objet d'un document de synthèse disponible par ailleurs et dans lequel sont développées les notions exposées ici.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui □ Non □

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui □ Non □

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui □ Non □

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension □
- présentation □
- autre □

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?

.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution