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

MEILLEURES PRATIQUES POUR LA GESTION DES RISQUES SSI

Utilisation de la méthode EBIOS®
pour rédiger une cible de sécurité de produit

Version du 10 novembre 2004

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

Qu'est-ce qu'une cible de sécurité de produit ?

Une cible de sécurité (ST – *Security Target*), au sens de la norme ISO 15408 – critères communs pour l'évaluation de la sécurité des technologies de l'information, est "un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une TOE identifiée" (la TOE – *Target Of Evaluation* est la cible d'évaluation, c'est-à-dire le produit étudié).

Il s'agit d'un document au contenu normé, qui peut servir de cahier des charges raffinant le contenu d'un profil de protection (PP) et qui peut aussi être évalué. Cette ST propose notamment un raffinement justifié des exigences de sécurité formalisées dans le PP. Elle permet à l'utilisateur de la TOE de se rendre compte de l'adéquation de la TOE à ses besoins.

Hors du contexte de l'évaluation technique (évaluation de produit certifiée par la DCSSI), il est possible de rédiger des cahiers des charges SSI sous la forme de ST, essentiellement dans le but d'utiliser un canevas et une terminologie reconnus.

Quels sont les avantages de la méthode EBIOS pour la rédaction d'une ST de produit ?

Une ST de produit doit être parfaitement complète et cohérente. Sa rédaction nécessite donc un travail rigoureux, mais la norme ne propose aucune méthode pour le réaliser. EBIOS permet de fournir tous les éléments nécessaires à la rédaction d'une ST, tout en garantissant leur cohérence. Elle offre de surcroît plusieurs avantages :

- la pertinence des objectifs de sécurité couvrant des menaces, hypothèses, règles de politique de sécurité et exigences de sécurité,
- la justification des objectifs et des exigences à l'aide de l'appréciation des risques SSI,
- l'exhaustivité de l'étude grâce à sa démarche structurée,
- l'implication des parties prenantes (Direction, maîtrise d'ouvrage, maîtrise d'œuvre, utilisateurs…).

Comment rédiger une ST de produit en utilisant EBIOS ?

Une solution efficace pour rédiger une ST consiste à :

- réaliser une étude EBIOS (sur un périmètre qui sera celui de la ST) en raffinant les exigences de sécurité,
- rédiger un PP et le faire valider sur la base de l'étude,
- extraire les données nécessaires dans l'étude (une grande partie de l'étude),
- rédiger l'introduction (identification de la ST et vue d'ensemble),
- réorganiser les objectifs de sécurité (à classer selon leur portée),
- réorganiser les exigences de sécurité (à classer selon leur portée),
- rédiger les annonces de conformité au PP.

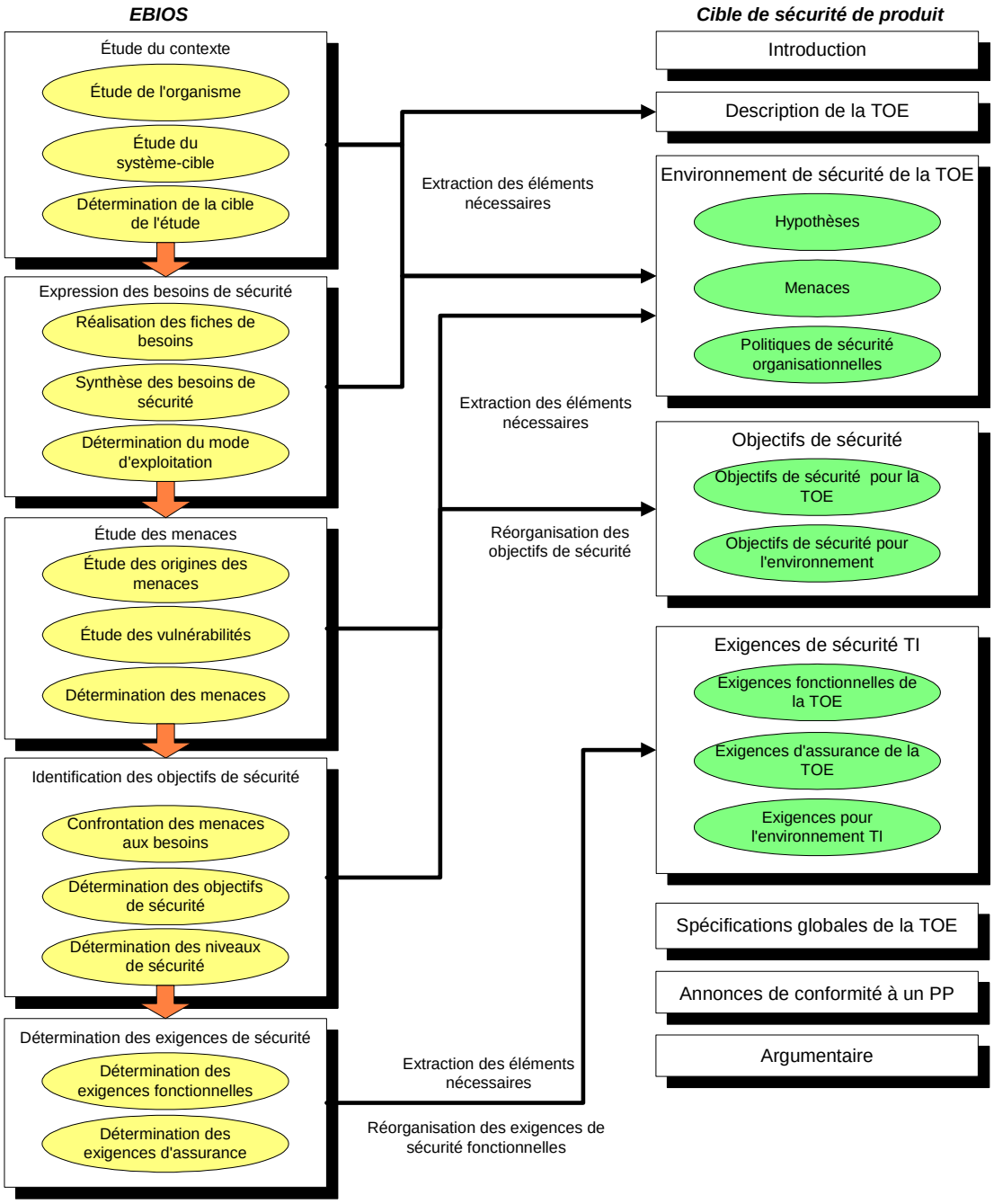
Pour cela, les activités de la méthode EBIOS sont utilisées de la manière suivante :

Activités EBIOS	Mise en œuvre dans le but de rédiger une ST de produit
ÉTAPE 1 Étude du contexte	En résumé : l'étude du contexte n'est axée que sur les informations nécessaires à la rédaction d'une cible de sécurité
1.1 – Étude de l'organisme	Il peut être utile de décrire les organismes ou types d'organismes dans lesquels le produit de sécurité est voué à être utilisé afin de définir des hypothèses d'environnement. Néanmoins, cette activité n'est généralement pas utilisée.
1.2 – Étude du système-cible	L'accent est mis sur le recueil des éléments nécessaires à la rédaction d'une ST : - présentation de la TOE et description fonctionnelle, - liste des éléments essentiels, - liste des hypothèses, - liste des règles de sécurité. Les autres éléments de cette activité ne devraient être étudiés que s'ils enrichissent la liste précédente.
1.3 – Détermination de la cible de l'étude de sécurité	Cette activité doit être détaillée et complète, bien qu'on ne s'intéresse généralement qu'aux entités techniques de types logiciels, matériels et réseaux.
ÉTAPE 2 Expression des besoins de sécurité	En résumé : les besoins de sécurité sont déterminés selon une échelle de besoins simple
2.1 – Réalisation des fiches de besoins	Les critères de sécurité, l'échelle de besoins et les impacts choisis doivent être simples, par exemple en définissant : - les trois critères de sécurité habituels (disponibilité, intégrité et confidentialité), - éventuellement un ou deux impacts (essentiellement liés à la perte de fiabilité des mécanismes), - une échelle binaire.
2.2 – Synthèse des besoins de sécurité	La synthèse des besoins de sécurité peut être réalisée directement sans passer par les fiches de besoins de sécurité unitaires.

Activités EBIOS	Mise en œuvre dans le but de rédiger une ST de produit
ÉTAPE 3 Étude des menaces	En résumé : l'étude des menaces est détaillée
3.1 – Étude des origines des menaces	L'activité doit être détaillée et complète. La caractérisation des méthodes d'attaque et des éléments menaçants doit être particulièrement claire et précise. Le potentiel d'attaque de chaque élément menaçant doit être indiqué, explicité et justifié. La liste justifiée des méthodes d'attaque non retenues doit être réalisée.
3.2 – Étude des vulnérabilités	Les vulnérabilités peuvent être issues des bases de connaissances de la méthode EBIOS, mais d'autres référentiels, plus techniques et plus détaillés sont généralement utilisés. La détermination des niveaux de vulnérabilité n'est utile que pour hiérarchiser les menaces dans la suite de l'étude.
3.3 – Formalisation des menaces	Cette activité doit être claire (à des fins de communication) et précise. Il est préférable de formuler des menaces unitaires, homogènes, spécifiques (une vulnérabilité par menace) et conformes aux profils de protection et ST existants.
ÉTAPE 4 Identification des objectifs de sécurité	En résumé : les risques explicitent les conséquences des menaces, les risques résiduels doivent "disparaître" au profit de modifications du contexte
4.1 – Confrontation des menaces aux besoins	Les risques doivent être identifiés et formulés de manière uniforme sur la base de la formulation des menaces. Ces risques pourront être intégrés dans la ST à la place des menaces (moins précises concernant les conséquences).
4.2 – Formalisation des objectifs de sécurité	La rédaction des objectifs de sécurité doit être claire, précise et uniforme afin de les justifier par leur contenu. Les objectifs de sécurité doivent être classés en deux catégories : - ceux portant sur la TOE, - ceux portant sur l'environnement de la TOE. Les éventuels risques résiduels identifiés doivent faire l'objet de modification du contexte (essentiellement dans l'activité 1.2) de telle sorte qu'il n'y ait plus de risque résiduel à ce niveau de l'étude. La démonstration de couverture des éléments de l'étude par les objectifs de sécurité doit être détaillée.
4.3 – Détermination des niveaux de sécurité	Les niveaux de sécurité doivent être explicites et dûment justifiés.

Activités EBIOS	Mise en œuvre dans le but de rédiger une ST de produit
ÉTAPE 5 Détermination des exigences de sécurité	En résumé : .
5.1 – Détermination des exigences de sécurité fonctionnelles	Les exigences de sécurité fonctionnelles devraient être issues de l'ISO 15408 ou créées selon les préconisations contenues dans la norme et raffinées pour que les spécifications soient directement applicables. Les éventuels risques résiduels identifiés doivent faire l'objet de modification du contexte (essentiellement dans l'activité 1.2) de telle sorte qu'il n'y ait plus un seul risque résiduel à ce niveau de l'étude. Les exigences de sécurité doivent être classées en deux catégories : - celles portant sur la TOE, - éventuellement celles portant sur l'environnement de la TOE. La démonstration de couverture des objectifs de sécurité par les exigences de sécurité fonctionnelles doit être détaillée.
5.2 – Détermination des exigences de sécurité d'assurance	Les exigences de sécurité d'assurance devraient être issues de l'ISO 15408 ou créées selon les préconisations contenues dans la norme. L'argumentaire relatif aux exigences de sécurité d'assurance doit être détaillé.

En résumé, les données exploitables sont les suivantes :



(pour tout complément d'information : ebios.dcssi@sgdn.pm.gouv.fr)