



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 spécifique de la méthode EBIOS®
pour rédiger un profil de protection

Version du 8 février 2005

Qu'est-ce qu'un profil de protection ?

Un profil de protection (PP), 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 valables pour une catégorie de TOE, indépendamment de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs" (la TOE – *Target Of Evaluation* est la cible d'évaluation, c'est-à-dire le système étudié).

Il s'agit d'un document au contenu normé, qui peut servir de cahier des charges auquel il convient de répondre par une cible de sécurité. Cette cible propose une couverture justifiée des exigences de sécurité formalisées dans le PP.

Hors du contexte de l'évaluation de produit (évaluation certifiée par la DCSSI), il est possible de rédiger des cahiers des charges SSI sous la forme de PP, essentiellement dans le but d'utiliser un canevas et une terminologie reconnus. Il est même possible d'utiliser ce canevas pour des systèmes d'information particuliers, alors que la norme n'évoque qu'une utilisation pour des produits de sécurité avec des spécifications génériques.

Quels sont les avantages de la méthode EBIOS pour la rédaction d'un PP ?

Un PP doit être parfaitement complet et cohérent. 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'un PP, tout en garantissant leur cohérence. Elle offre de surcroît plusieurs avantages :

- la pertinence des objectifs de sécurité couvrant des menaces (pour le produit, le SI ou l'organisme), hypothèses et règles de politique de sécurité, ainsi que des exigences de sécurité,
- la justification des objectifs et des exigences de sécurité 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...), dans le cas d'un SI particulier.

Comment rédiger un PP en utilisant EBIOS ?

Une solution efficace pour rédiger un PP consiste à :

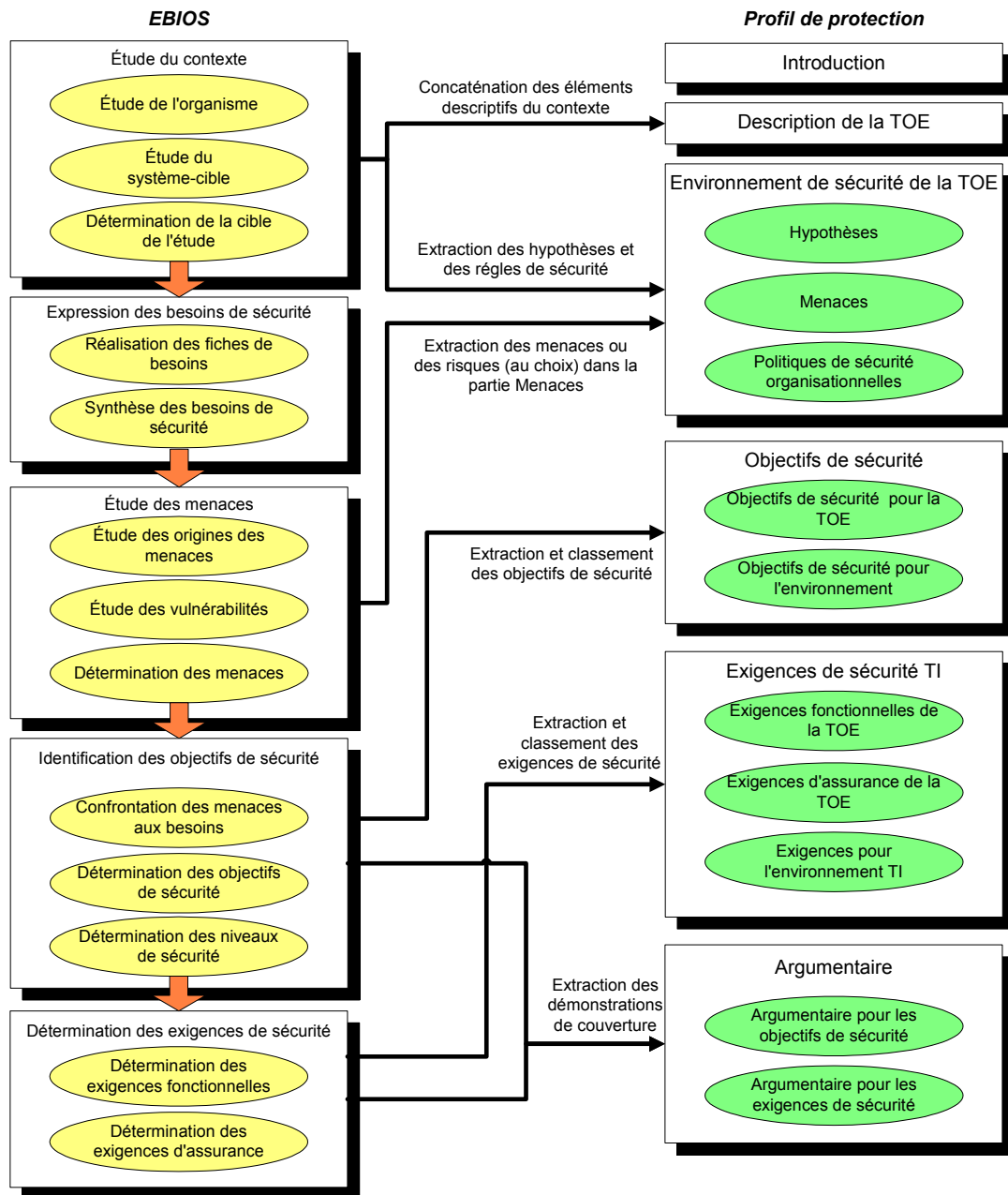
- réaliser une étude EBIOS sur le périmètre concerné par le PP,
- extraire les données nécessaires dans l'étude (une grande partie de l'étude),
- rédiger l'introduction (identification du PP et vue d'ensemble),
- réorganiser les objectifs de sécurité (à classer selon leur portée),
- réorganiser les exigences de sécurité (à classer selon leur portée).

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

Activités EBIOS	Mise en œuvre dans le but de rédiger un PP
<p align="center">ÉTAPE 1</p> <p align="center">Étude du contexte</p>	<p align="center">En résumé : l'étude du contexte est approfondie et sera complétée tout au long des travaux</p>
<p>1.1 – Étude de l'organisme</p>	<p>Cette activité doit permettre de préciser le contexte théorique de l'étude.</p>
<p>1.2 – Étude du système-cible</p>	<p>Cette activité doit être détaillée, notamment pour la description fonctionnelle du système-cible. Il importe que celle-ci soit claire, concise et aussi standardisée que possible.</p> <p>Il est important de considérer les interfaces avec les autres systèmes d'information.</p> <p>Les éléments essentiels doivent être listés et décrits, éventuellement en extrapolant l'utilisation qui sera faite du système-cible.</p> <p>Seules les hypothèses et les règles de sécurité doivent être utilisées (et non les contraintes, références réglementaires et enjeux, bien que ceux-ci puissent être utilisés pour compléter la description du système-cible). Elles pourront être enrichies tout au long des travaux.</p>
<p>1.3 – Détermination de la cible de l'étude de sécurité</p>	<p>Cette activité doit être aussi détaillée que les spécifications le permettent.</p>
<p align="center">ÉTAPE 2</p> <p align="center">Expression des besoins de sécurité</p>	<p align="center">En résumé : l'expression des besoins de sécurité est simple</p>
<p>2.1 – Réalisation des fiches de besoins</p>	<p>L'activité doit permettre de réaliser une échelle de besoins simple (peu de niveaux, voire une échelle binaire) en termes de disponibilité, intégrité, confidentialité...</p> <p>Les impacts ne doivent pas être étudiés, à moins que le contexte d'utilisation du système-cible soit suffisamment connu.</p>
<p>2.2 – Synthèse des besoins de sécurité</p>	<p>Cette activité doit permettre de déterminer les besoins de sécurité en dessous desquels il est inacceptable de descendre en termes de disponibilité, intégrité, confidentialité...</p>
<p align="center">ÉTAPE 3</p> <p align="center">Étude des menaces</p>	<p align="center">En résumé : l'étude des menaces est détaillée et peut ne pas traiter de l'opportunité</p>
<p>3.1 – Étude des origines des menaces</p>	<p>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, explicite et justifié.</p> <p>La liste justifiée des méthodes d'attaque non retenues doit être</p>

Activités EBIOS	Mise en œuvre dans le but de rédiger un PP
	réalisée.
3.2 – Étude des vulnérabilités	<p>Cette activité doit être détaillée et complète.</p> <p>Toutes les vulnérabilités potentielles doivent être relevées, mais il n'est pas nécessaire d'en déterminer un niveau.</p>
3.3 – Formalisation des menaces	<p>Cette activité doit être claire (à des fins de communication) et précise.</p> <p>Il est préférable de formuler des menaces unitaires et spécifiques (une vulnérabilité par menace).</p> <p>La hiérarchisation des menaces n'est pas nécessaire.</p>
<p>ÉTAPE 4</p> <p>Identification des objectifs de sécurité</p>	<p>En résumé : l'identification des objectifs de sécurité démontre que les risques sont parfaitement couverts, que les hypothèses et règles de sécurité sont prises en compte, et permet de statuer sur les niveaux de sécurité</p>
4.1 – Confrontation des menaces aux besoins	<p>Les risques doivent être identifiés et formulés de manière uniforme.</p>
4.2 – Formalisation des objectifs de sécurité	<p>La rédaction des objectifs de sécurité doit être claire, précise et uniforme afin de les justifier par leur contenu. Ils peuvent utilement être classés en "objectifs de sécurité pour la TOE" et "objectifs de sécurité pour l'environnement".</p> <p>La prise en compte des hypothèses et règles de sécurité doit être démontrée.</p> <p>Les éventuels risques résiduels doivent faire l'objet d'hypothèses excluant leurs conditions de réalisation afin qu'il n'en reste aucun.</p>
4.3 – Détermination des niveaux de sécurité	<p>Les niveaux de sécurité doivent être explicites et dûment justifiés.</p>
<p>ÉTAPE 5</p> <p>Détermination des exigences de sécurité</p>	<p>En résumé : les exigences de sécurité fonctionnelles et d'assurance pourront directement constituer des règles de sécurité de la PSSI, elles seront éventuellement complétées par d'autres règles, élaborées en réponse à des besoins non couverts par l'étude EBIOS.</p>
5.1 – Détermination des exigences de sécurité fonctionnelles	<p>Les exigences de sécurité fonctionnelles doivent généralement être issues de l'ISO 15408 (partie 2).</p> <p>Le niveau des exigences de sécurité fonctionnelles doit notamment dépendre des niveaux de résistance.</p> <p>Les éventuels risques résiduels doivent faire l'objet d'hypothèses excluant leurs conditions de réalisation afin qu'il n'en reste aucun.</p>
5.2 – Détermination des exigences de sécurité d'assurance	<p>Les exigences de sécurité d'assurance doivent généralement être issues de l'ISO 15408 (partie 3).</p>

En résumé, les données exploitables sont les suivantes :



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