

Pilotage de la PSSI en DR12

M. Culioli

M.Libes

M .Kourilsky

Février- Octobre 2008

DR12 - Organisation de la CRSSI

Quelques chiffres :

101 structures opérationnelles de recherche

CRSSI : 3 ingénieurs

- Michel Kourilsky
- Martine Culioli
- Maurice Libes

CSSI :

- 40 « confirmés » = à nommer par décision
- Pour les unités restantes = sollicitation du DU
- Objectif = 1 CSSI par « entité »

PSSI - Principales actions réalisées ou engagées

Actions de communication et de sensibilisation

Publics visés :

- DU

- Réunion annuelle des DU (déc. 2007)
- Séminaire nouveaux DU (avril 2008)

- CSSI et Informaticiens de laboratoire

- séance plénière (2007)
- présentation avancement PSSI pilote
- mai 2008 – réunion réseau des ASR régionaux CESAR

PSSI - Principales actions réalisées ou engagées

Actions opérationnelles

- Fév. 2008 – Formation à la méthode EBIOS (formateur : P. Tourron Univ. Méditerranée)
- recrutement d'un stagiaire : étudiant d'un master 2 de Sécurité des Systèmes d'Information (Univ. Toulon)
- Avril 2008 – DR12 – SSI – Étude ciblée utilisant EBIOS
- Mai 2008 – choix du Labo pilote LMA de M. Culioli pour démarrer le projet de PSSI pilote (ERR sur DR12)

En parallèle : participation de M. Libes au groupe de travail sur la PSSI de l'Université de la Méditerranée

Organisation du projet PSSI en DR12

Choix d'EBIOS pour l'analyse de risque :

- Cohérence avec la méthode utilisée par l'université
- Formateur EBIOS régional
- what else?

Création d'un Comité de pilotage pour la PSSI du LMA

- 9 personnes : Direction + Chercheurs & IT +CRSSI
- Comité restreint : 4 personnes (CRSSI + stagiaire)
- Experts métiers (entretiens)

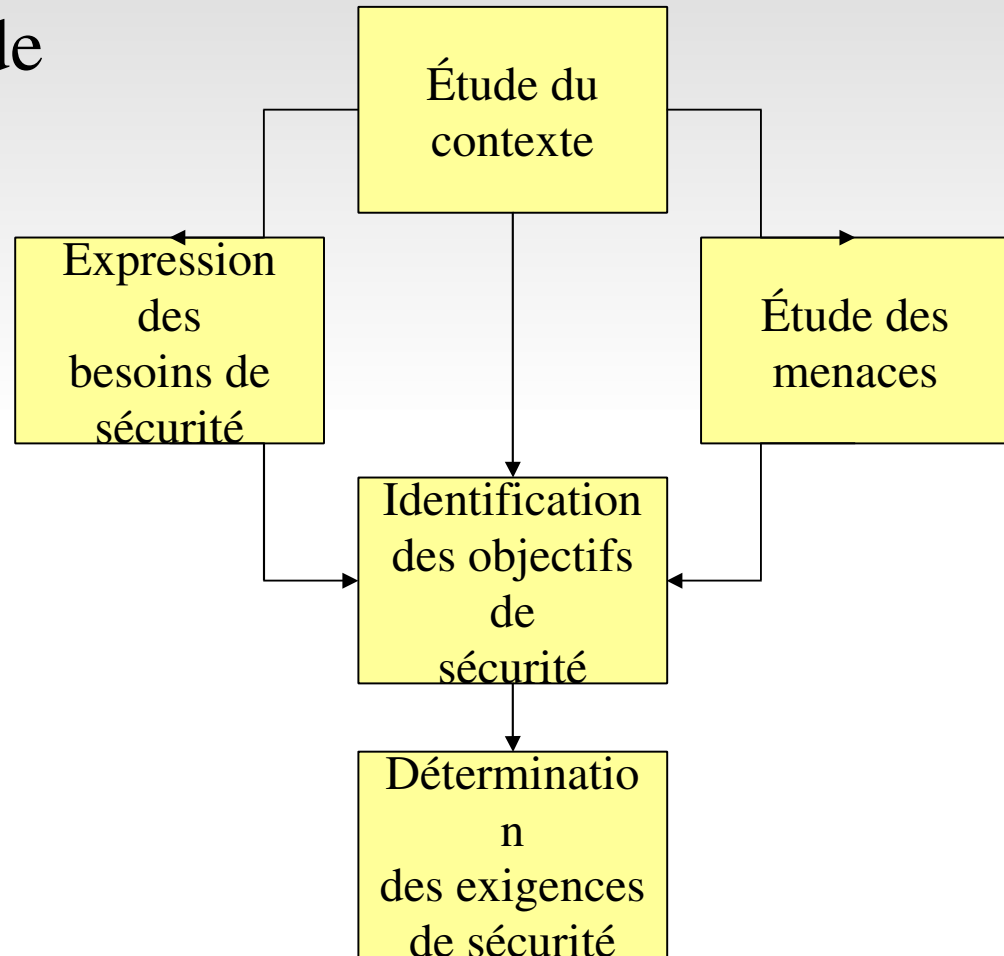
Méthode EBIOS

Expression des Besoins et Identification des Objectifs de Sécurité

- Elaborée par la DCSSI, la méthode EBIOS permet d'apprécier et de traiter les risques relatifs à la SSI.
- Elle est bien documentée (guides sur le site de la DCSSI) et dispose d'un outil logiciel libre permettant de consigner les données de l'étude et produire les documents de synthèse
- Elle propose des étapes qui permettent une analyse exhaustive

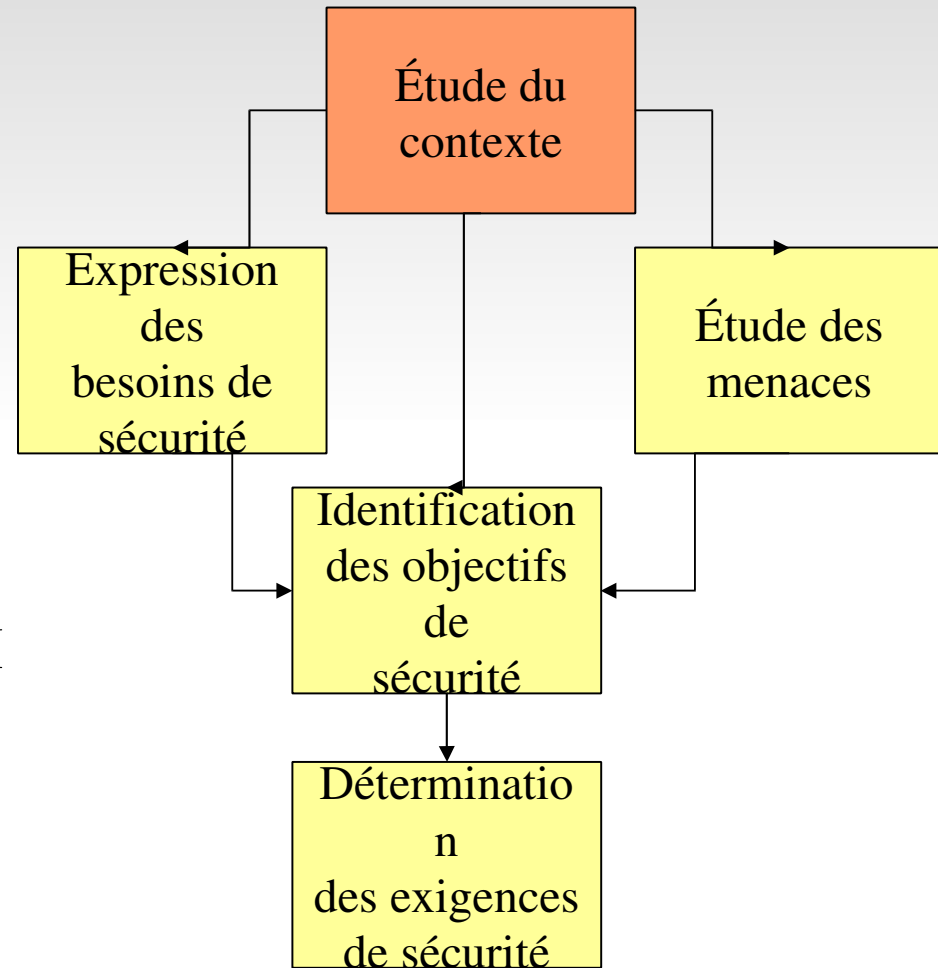
Méthode EBIOS - déroulement au LMA

- Utilisation de la méthode EBIOS
- 5 étapes
- Comité restreint
 - Analyse et Etude du système, et Propositions
- Comité de pilotage
 - Vérification et validation



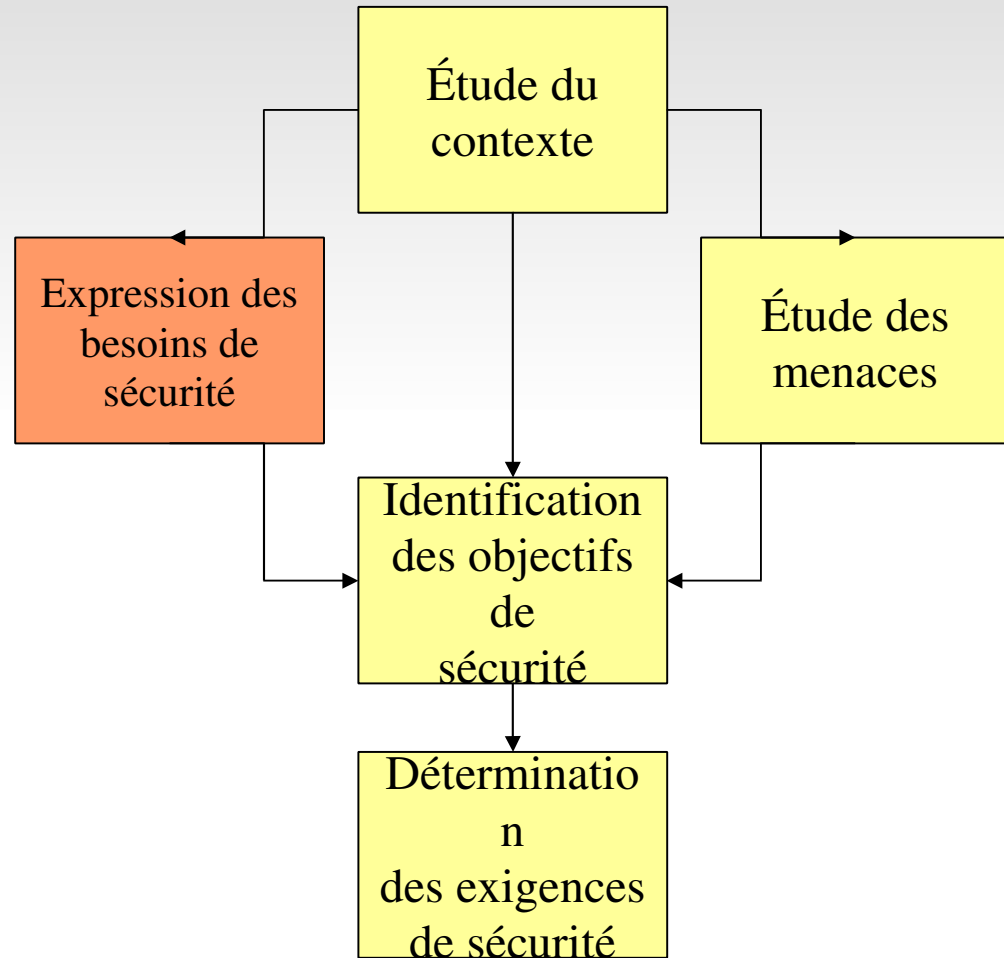
Étude du contexte

- *Étude de l'organisme*: missions, valeurs propres, axes stratégiques, description fonctionnelle.
- *Étude du système-cible*: périmètre, enjeux, **éléments essentiels** (*données et fonctions qu'on veut protéger*)
- Détermination de la cible de l'étude: **entités** composantes du SI (*les locaux, les matériels, les logiciels..*)



Expression des besoins de sécurité

- Etablissement d'une échelle estimative des besoins en terme de *disponibilité, intégrité, confidentialité*
- Audition des experts métiers : quels sont leurs besoins pour éviter les impacts retenus?
- Synthèse des besoins de sécurité

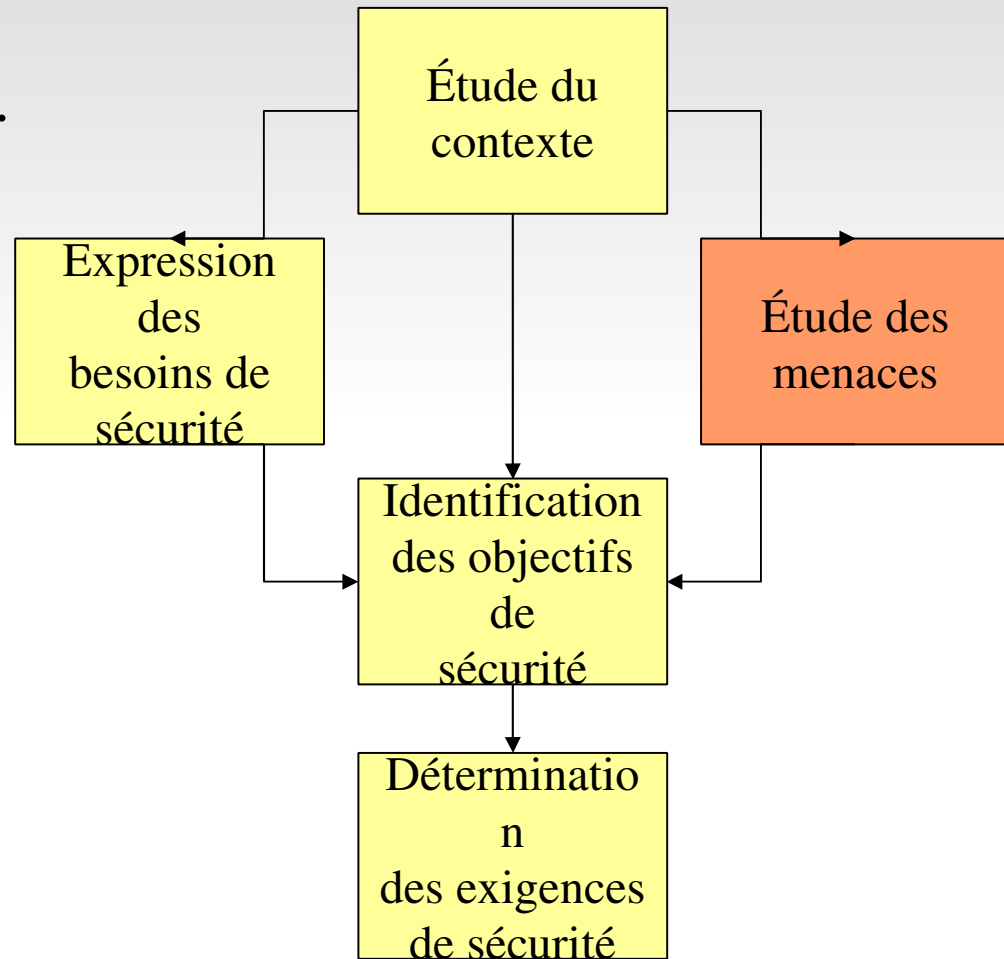


Expression des besoins de sécurité

- L'étape « expression des besoins » est en cours, elle nécessite *l'audition d'experts métier*.
 - Etablir une échelle des besoins en terme de *disponibilité, intégrité, confidentialité,*
 - Déterminer les impacts significatifs pour le laboratoire (*perte financière, perte d'image de marque, etc...*)
 - évaluer avec cette échelle et en fonction des impacts retenus, les besoins de sécurité pour chaque élément essentiel du laboratoire

Etude des menaces

- Recensement des scénarios pouvant porter atteinte au SI.
- Nécessite la définition de 3 données :
 - Méthode d'attaque
 - Vulnérabilités des entités
 - Niveau de vulnérabilité



Etat d'avancement :

définition des menaces

- L'étape « menaces » a été réalisée par le groupe restreint. Nous avons :
 - sélectionné *les méthodes d'attaque* (liste fournie par la méthode); par ex: incendie, écoute passive...
 - sélectionné les *vulnérabilités* du SI (liste fournie que nous avons quelquefois modifiée); *par ex: pas de portes coupe-feu, bureaux ouverts...*
 - évalué des *niveaux de vulnérabilité* (degré de plausibilité des vulnérabilités)
 - formulé les *menaces*.

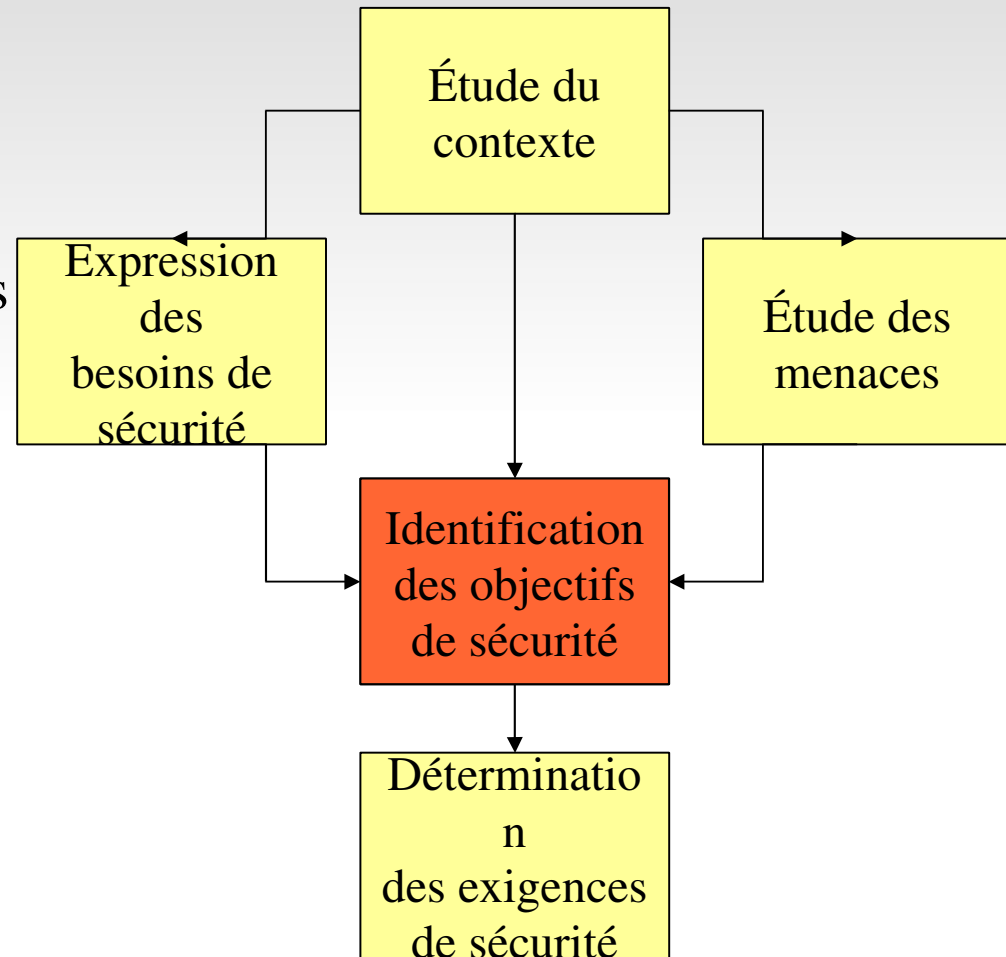
Etat d'avancement : définition des menaces

- Exemples de rédaction des menaces (*vulnérabilité exploitée par une attaque et sa probabilité d'occurrence sur une entité*) :
 - *L'absence de cloisonnement anti-feu dans les locaux du LMA pourrait aggraver les conséquences d'un incendie, déclenché de manière délibérée ou accidentelle, en facilitant sa propagation*
 - *Le faible contrôle d'accès aux bureaux et salles de manipulation du LMA peut permettre à un individu non autorisé d'effectuer des écoutes passives (accès à des pc non protégés, pose de matériel d'écoute, etc.).*

A venir: identification des objectifs de sécurité

- *Etape « identification des objectifs de sécurité »*

- Déterminer les risques (confronter menaces et besoins de sécurité)
- exprimer et hiérarchiser les risques (-> plan d'action)
- déterminer les objectifs de sécurité: un objectif peut couvrir plusieurs risques



Bilan du projet : le temps

- Réunions groupe restreint (4 personnes)
 - 12 réunions, temps passé: 36 heures
 - 3 auditions experts : 9heures
- Réunions groupe projet (9 personnes)
 - 3 réunions, temps passé: 6 heures
- Projet à mi-parcours, estimation du temps de réalisation du projet (dont auditions):
 - 180 h/h en groupe restreint
 - 160 h/h en groupe projet

NB : l'aide du stagiaire a été déterminante : saisie des données dans le logiciel Ebios, formulation des menaces etc...

Bilan et conclusion : intérêts

- démarche de la méthode ebios intéressante intellectuellement :
 - l'étude du contexte, des valeurs propres du labo, du périmètre,
 - l'inventaire des « éléments essentiels » (fonctions et données du SI)
 - l'inventaire des entitéssont des analyses fondamentales dans l'étude du SI du Labo
- on réfléchit **POUR UNE FOIS** à ce qui est important pour le laboratoire en terme de sécurité

Bilan et conclusion : intérêts

- audit du personnel : on fait exprimer les membres du laboratoire sur leurs besoins en terme de « D » « I » « C » sur les données et fonctions qu'ils utilisent
- on inventorie et hiérarchise
 - les impacts (*atteinte à la vie privée, respect de la législation...etc*)
 - les vulnérabilités (*faible contrôle d'accès, absence de pare feu...*)
 - les méthodes d'attaques (*vol, intrusions..*)

Difficultés rencontrées

- Ce n'est pas notre métier : on tâtonne,
 - planification épisodique et fragmentaire des réunions
 - les notions de la méthode ont nécessité des débats et réflexions laborieux : *formulation des menaces, probabilité d'occurrence, niveaux de vulnérabilités et de risque...*
- La mobilisation du groupe projet est difficile : *documents envoyés avant réunion non lus, disponibilité faible des membres du groupe*
- Faible sensibilisation des différents acteurs, faible soutien et pilotage de l'opération... nécessiterait une véritable « gestion de projet » pour faire travailler les gens ensemble

la suite?

- Comment terminer ? comment exploiter l'analyse de risque EBIOS ?... pour parvenir à la rédaction d'une PSSI d'unité
- méthode trop lourde à déployer sur la centaine de laboratoires de la délégation *compte tenu des moyens engagés*
- nécessité d'une simplification de la démarche :
 - besoins de sécurité sur éléments essentiels (données et fonctions des laboratoires)
 - menaces sur les entités (locaux, logiciels, matériels, personnes)
 - impacts retenussont vraisemblablement communs à tous les laboratoires : inutiles de refaire 100 fois les mêmes analyses
- Tronc commun et Les laboratoires devraient se focaliser sur leurs spécificités