ON-X Sécurité

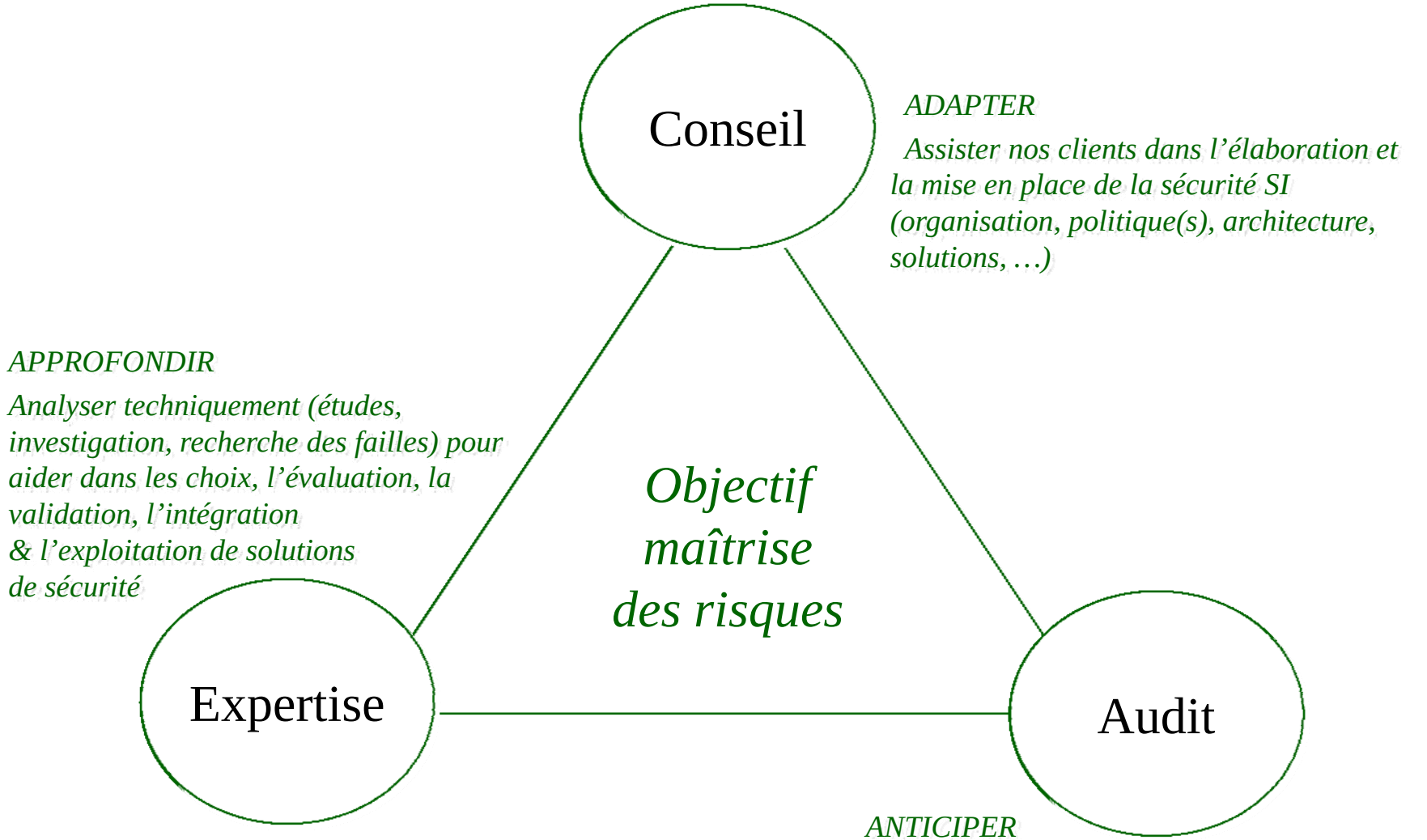
Des experts pour vous conseiller

Présentation d'une démarche de sécurisation du système d'information

[adaptée d'EBIOS]

EdelWeb

ON-X Sécurité - Nos trois types d'intervention



ADAPTER

Assister nos clients dans l'élaboration et la mise en place de la sécurité SI (organisation, politique(s), architecture, solutions, …)

APPROFONDIR

Analyser techniquement (études, investigation, recherche des failles) pour aider dans les choix, l'évaluation, la validation, l'intégration & l'exploitation de solutions de sécurité

ANTICIPER

Évaluer l'adéquation du niveau de sécurité des systèmes d'information par rapport aux enjeux des métiers de nos clients

Sujet - « Élaboration d'un plan de sécurité »

- **Objectif**
  - « On a un accident … la direction a décidé … , il faut protéger notre informatique ! »
  - Établir un état des lieux du niveau de sécurité compréhensible par les directions
  - Élaborer un plan de sécurité visant à améliorer la protection d'un **système d'information global EXISTANT « sans révolution »**
- **Contexte**
  - Ensemble complexe réunissant de très **nombreuses entités** du système d'information avec **des échanges** de plus en plus fréquent
  - **Actions de sécurité ponctuelles** (sécurisation de l'accès Internet, sauvegarde, …) - Résultats en général mal perçus par les utilisateurs
  - **Sensibilisation globale faible** face aux besoins de confidentialité, d'intégrité et d'opposabilité

    « il n'y a pas tant d'accident que cela … » ; « la sécurité est l'affaire de la technique, l'informatique s'en occupe … »
  - Risques informatiques **sans lien** avec les risques opérationnels
  - **Budget limité** sachant que l'étude ne sera pas une finalité !

Écueils dans la pratique d'EBIOS

- **Liste des informations et fonctions très grande et pas toujours connue**
  - Il n'existe pas parfois de personne ayant une vision globale du système d'information
  - Difficulté des interlocuteurs à considérer un bien sensible suffisamment protégé
- **Périmètre parfois difficile à délimiter**
  - Responsabilités superposées (système d'information, métiers, projets)
  - Le contexte est en constante évolution
  - De nombreux échanges rend la frontière de l'étude floue

  « Doit-on ou non prendre en compte les moyens de sécurité en place ? »
- **Démarche longue accompagnée d'une imprégnation difficile des concepts nos clients**
  - Les interlocuteurs confondent menaces, vulnérabilités, attaques, risques
  - Les métriques sont mal perçues
  - L'étude se transforme parfois en « usine à gaz » ou en résultat d'expert

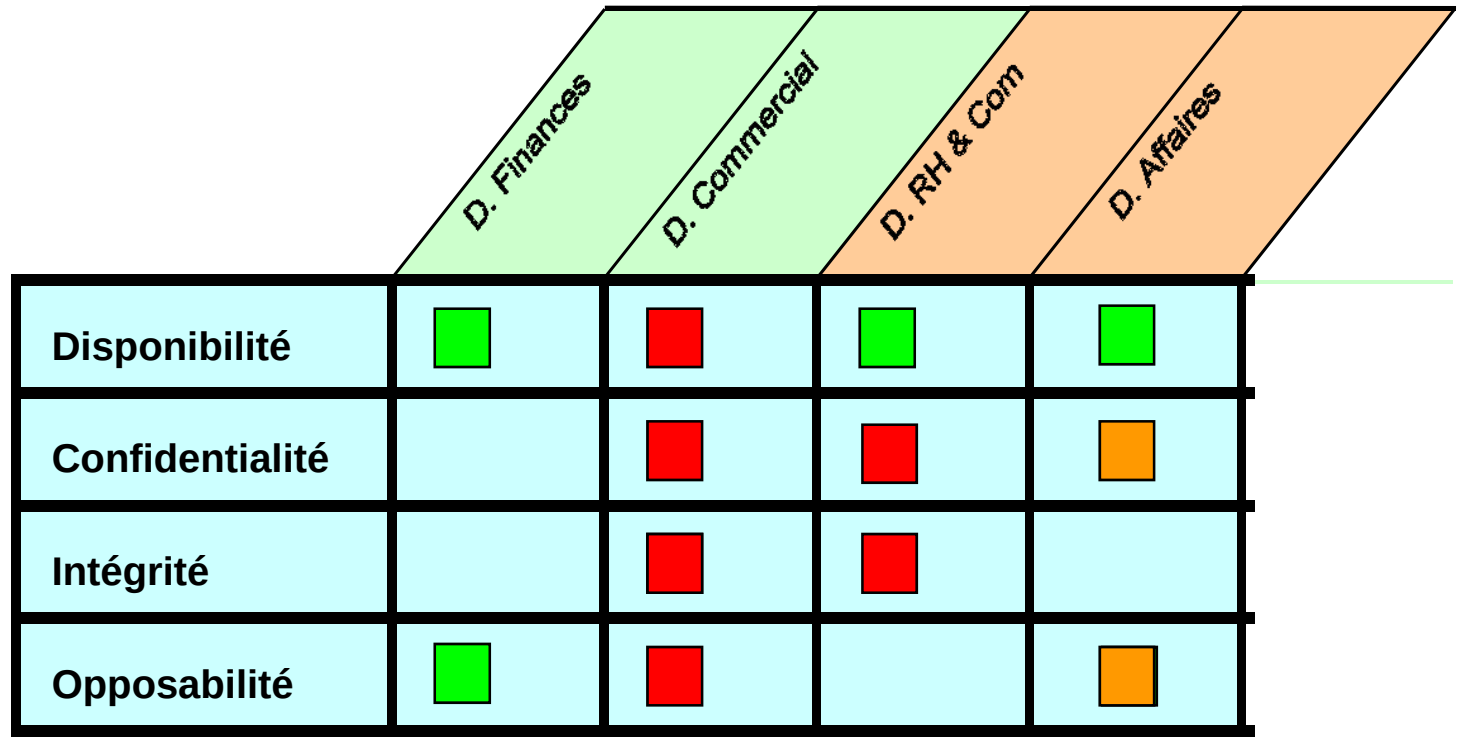
Idée fausse : « L'application de la démarche va nous apporter la solution !!! »

Principes de la méthode utilisée (1)

- **Disposer au plus vite d'une formalisation et de l'identification des attentes**
  - utiliser l'expérience du marché pour formaliser les invariants et cibler les éléments spécifiques (et les questions structurantes)
  - ➔ GPSSI (?) après le logiciel GPC
- **Dissocier les approches « système » et « opérationnelle »**
  - Les moyens communs [messagerie, serveurs bureautiques, accès internet, etc.]
    - ➔ problématiques « semi » - standard
  - Les moyens et pratiques des « métiers »
    - ➔ problématiques spécifiques auprès des maîtrises d'ouvrage
- **Utiliser comme référence le niveau offert en standard par l'informatique**
  - Métrique simple = Raisonner par différence en identifiant les besoins supplémentaires
  - Analyser ensemble l'origine des risques qu'ils redoutent sans rechercher l'exhaustivité
  - ➔ Identification de besoins réellement justifiés par des enjeux
  - ➔ Identification des contradictions

EdelWeb

Exemple de résultats des besoins des métiers



Prioritaire

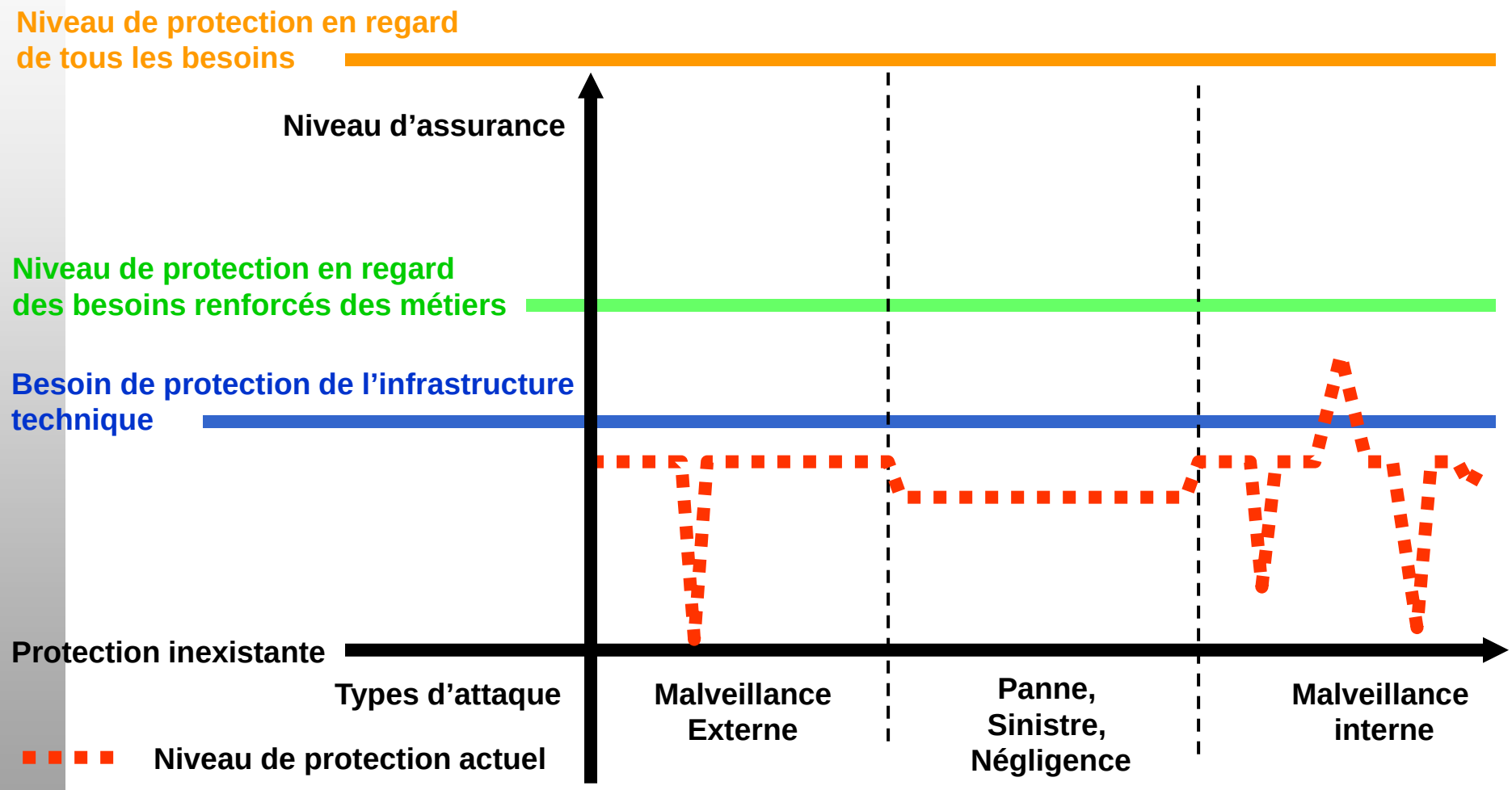
moins prioritaire

Renforcé

Standard

Standard
= service de base

Constat – État de la sécurité chez nos clients

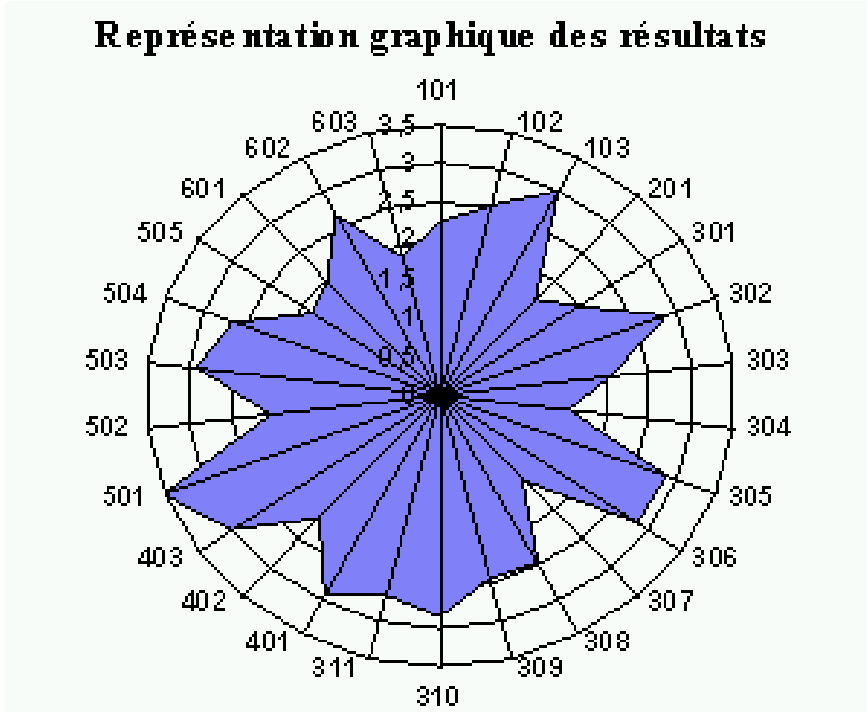


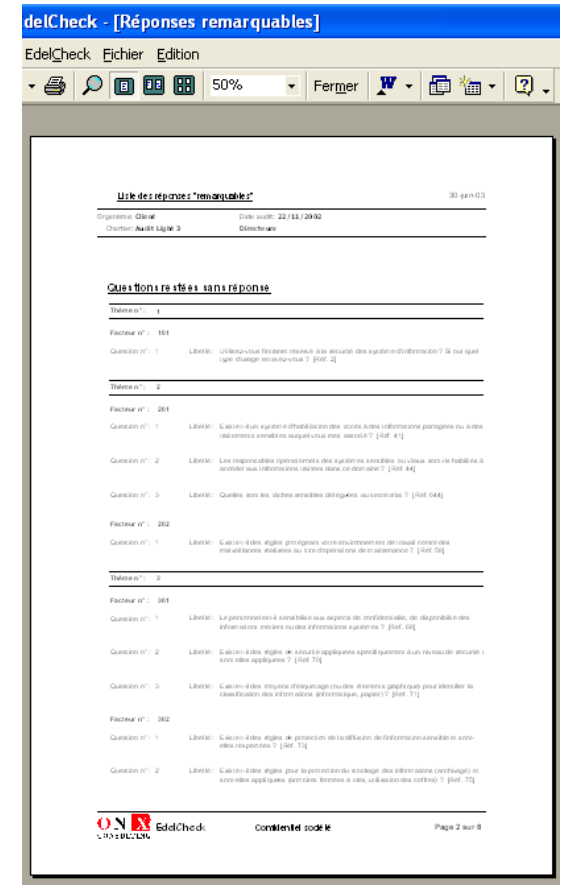
Principes de la méthode utilisée (2)

- **Audit du système d'information**
  - Utilisation de référentiel adapté en fonction des moyens choisis comme *norme* et des éléments redoutés par les métiers
- **Approfondir des analyses sur des entités sensibles du SI**
  - Qualification de solutions techniques sur lesquels reposent de réels enjeux
- **Relier les approches « système » et « métiers »**
  - Identification des écarts : besoins non (ou partiellement) satisfaits
  - En fonction du coût, finaliser les besoins pour décrire les objectifs de sécurité prioritaires
- **Justifier les exigences de sécurité en les rapprochant de scénarios de risque**
  - Reprendre les vulnérabilités en les pondérant par les objectifs initialement retenues ➔ Établir un plan de sécurité à partir de critères jugés objectifs
  - Chercher des solutions ➔ « Défense en profondeur »
- **Identifier clairement les risques résiduels acceptés afin de responsabiliser la direction**
  - Corollaire : niveau d'assurance pour la couverture du risque inacceptable

EdelWeb

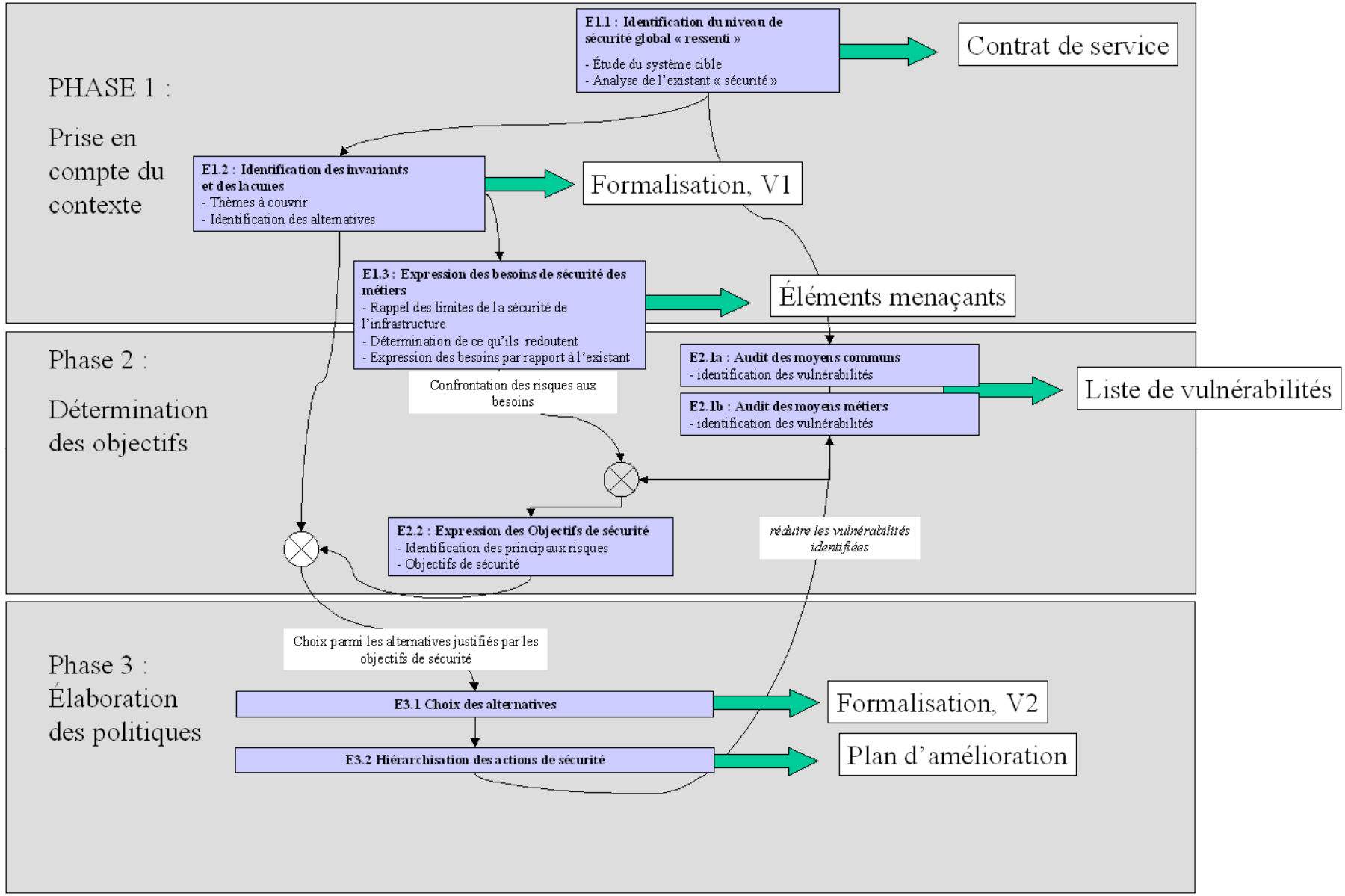
EdelCheck™ - Outillage d'audit restreint mais suffisant





EdelWeb

Présentation générale de la méthode



Forces de la méthode utilisée

- **La sécurité n'est pas un ensemble imposé de moyens techniques mais une réponse à des besoins exprimés (« organisme » et « métier »)**
- **Pragmatisme de la méthode qui considère que l'espace de solutions est limité**
- **Prise de conscience et implication des métiers**
  - **Comme faisant partie d'un ensemble**
  - **comme maîtres d'ouvrage des applications**
- **Occasion pour modéliser le SI**
- ***Plus classiquement : gradation des moyens, cohérence des mesures, implication des métiers dans la démarche, …***

Démultiplication des ressources
et la pérennité des réponses aux besoins

Jean OLIVE
Consultant manager
jean.olive@edelweb.fr

T: +33 1 40 99 29 63
www.edelweb.fr

EdelWeb