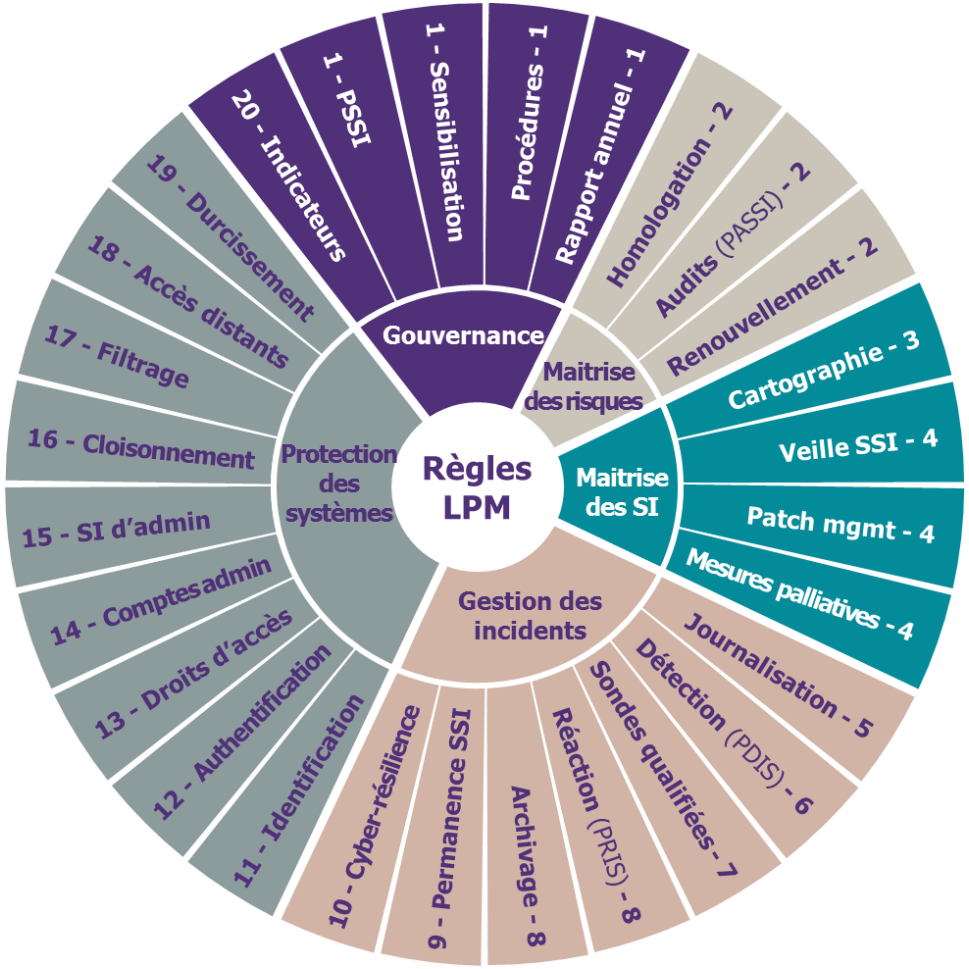
Sécuriser un SIIV : bilan financier

Etienne CAPGRAS, Wavestone

WAVESTONE

Club de la sécurité de l'information français

20 règles pour protéger les SI d'importance vitale et promouvoir les bonnes pratiques SSI



La LPM cherche à protéger les parties du SI des OIV jugées d'importance vitale : les SIIV

« systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population »

PASSI
Prestataires d'audit de la sécurité du système d'information

PDIS
Prestataires de détection des incidents de sécurité

PRIS
Prestataires de réponse à incidents

Un retour d'expérience s'appuyant sur un échantillon spécifique correspondant à nos interventions

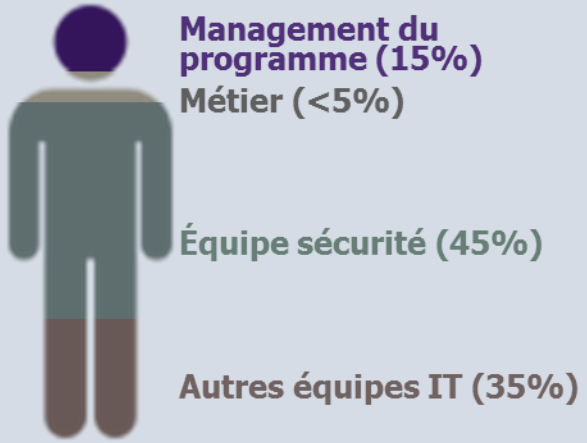
17 OIV grands comptes

35 donneurs d'ordre

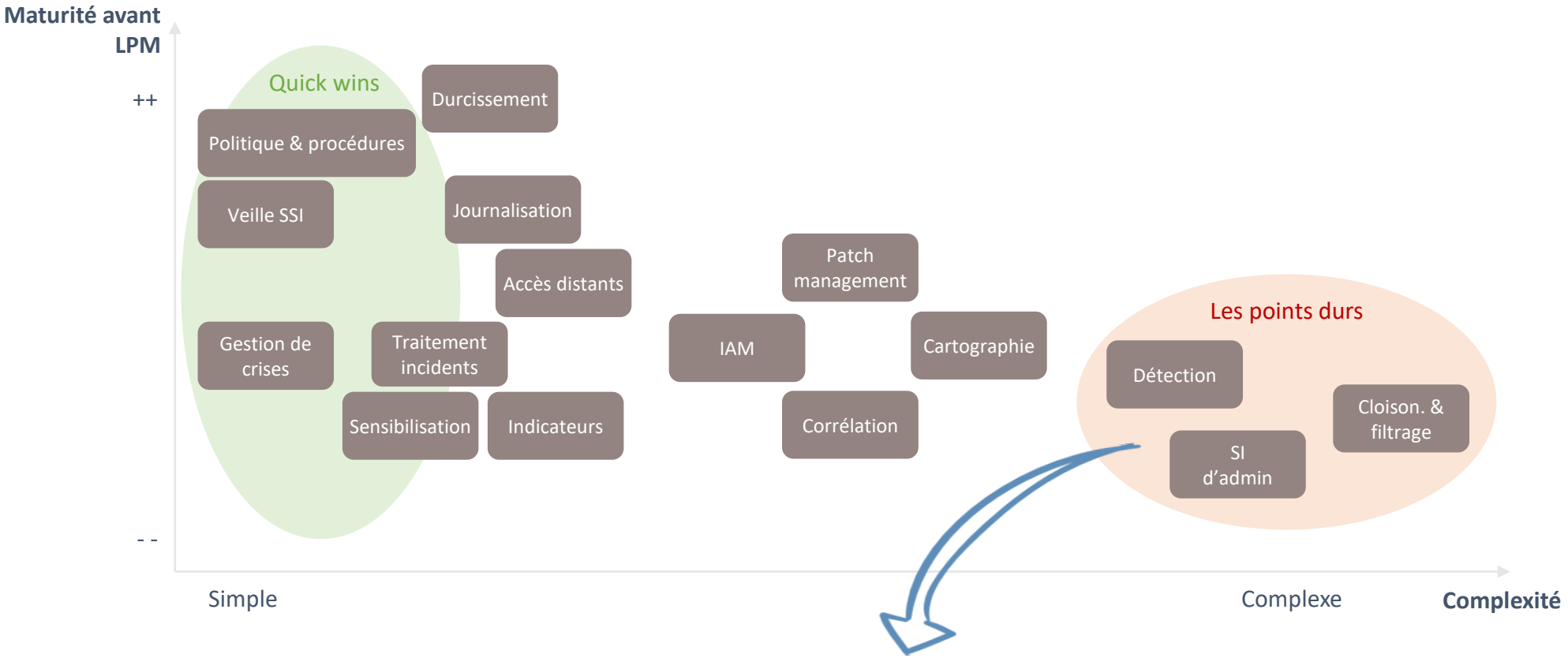
7 secteurs couverts

Des programmes de **3 à 4 ans**, pilotés par les **équipes sécurité** (RSSI), qui impliquent jusqu'à **une centaine d'acteurs** : dirigeants, sûreté, RSSI, conformité, métiers, DSI, achats, équipes IT, filière industrielle et automaticiens…

Une charge de 15 à 20 ETP répartie majoritairement entre sécurité et IT



Des sujets à la maturité et à la complexité variées



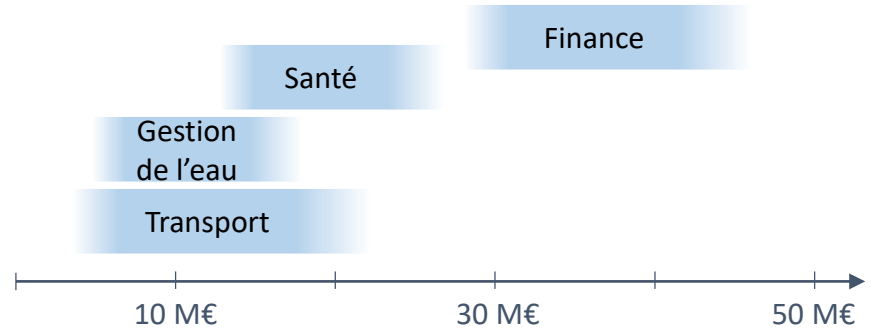
*Être au rendez-vous des **constructions budgétaires**, dès maintenant*

*Les macro-cibles sont ainsi définies **en amont des analyses de risques** et en composant avec un **marché pas encore structuré** autour de la LPM*

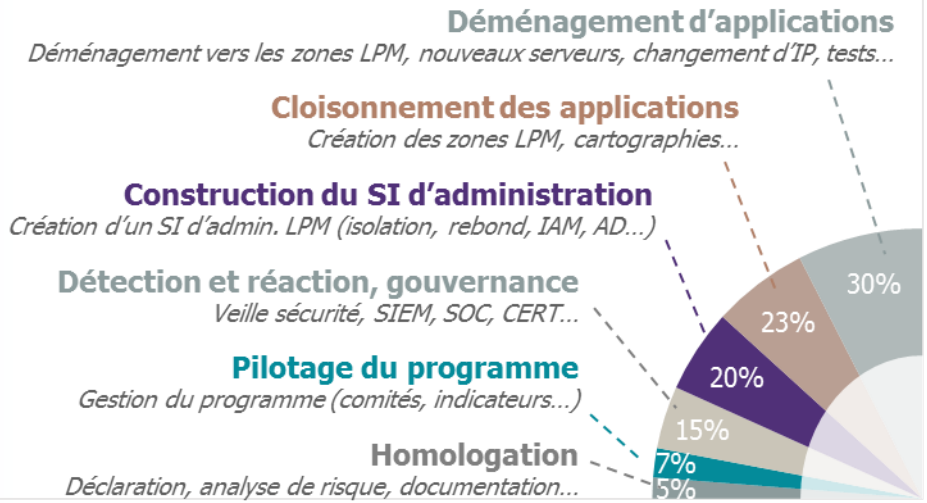
Club de la sécurité de l'information français

Quel coût pour un projet LPM ?

Répartition initiale des budgets de mise en conformité par secteur*



Répartition du budget par chantier



- Des **budgets initiaux très importants** de mise en conformité LPM, notamment en raison des incertitudes sur les règles au lancement du programme
- Les **budgets sont réajustés** progressivement à la baisse, au gré des arbitrages internes et de la clarification des règles (jusqu'à un facteur 2)
- Deux postures sont conjointement adoptées par les OIV
  - **Conformité** : application stricte des arrêtés comme tout projet de mise en conformité
  - **Optimisation** : les équipes sécurité élargissent le périmètre couvert pour augmenter plus largement le niveau de sécurité (SI d'administration, SOC, applications non SIIV mais critiques pour l'entreprise…) et l'intègrent dans un programme global
- Les équipes sécurité ne peuvent supporter seules le coût de mise en conformité et demandent des **budgets complémentaires aux DSI**, voire aux **Directions Générales**, qui exigent des optimisations de budget.

➔ **Des budgets qui vont se diluer dans les projets une fois lancés**

Comment se mettre en conformité efficacement ?

1. **Dresser la liste des SIIV**
   > Les applications IV représentent au maximum 3% du parc applicatif des OIV grands comptes
2. **Recenser les écarts et dessiner des premières cibles**
   > Macro-budget : ne pas attendre la stabilisation de la liste des SIIV, ne pas traiter règle par règle
3. **Favoriser la pratique à la théorie : POCs et pilotes !**
   > Audits à blanc, homologation sur SIIV pilote, mise en œuvre des mesures sur SIIV pilote
4. **Paralléliser les chantiers**
   > Pour tenir les délais et identifier les adhérences : guides de durcissement, PSSI, clauses contractuelles, etc.
5. **Tirer parti de la complémentarité des équipes**
   > De nombreux interlocuteurs mobilisés : opportunité d'actionner des leviers jusque-là souvent inaccessibles