12 décembre 2013

Gestion des comptes à privilèges

Bertrand CARLIER, Manager Sécurité de l'Information

bertrand.carlier@solucom.fr

solucom
management & IT consulting

Solucom, conseil en management et système d'information

- Cabinet de conseil indépendant

  coté sur NYSE Euronext

- Notre mission

  porter l'innovation au cœur des métiers

  cibler et conduire les transformations créatrices de valeur

  faire du SI un actif au service de la stratégie des entreprises

- Notre approche du conseil

The power of simplicity
«Ce qui est simple est fort»

- ✓ 20 ans d'existence
- ✓ ~ 1 200 collaborateurs
- ✓ 2/3 des entreprises du CAC 40 nous font confiance
- ✓ Une capacité d'intervention à l'international

« Solucom 2015 » :
devenir le 1er cabinet de conseil indépendant en France

Qui sommes-nous ?

Notre mission est d'accompagner nos clients dans la **maîtrise des risques** et la **conduite des projets** au **bénéfice des métiers**

Nos **convictions** :

1. **Prioriser** les risques en fonction des enjeux des métiers
2. **Faciliter** l'évolution des usages en centrant la sécurité sur l'information
3. Allier protection, **détection et réaction** pour faire face aux nouvelles menaces

Une conjugaison d'**expertises** de premier plan :

Stratégie, gouvernance et pilotage des risques

Continuité	Infrastructures	Sécurité applicative	Gestion des identités	Gestion opérationnelle	Audits et tests d'intrusions

Pilotage et réalisation des projets / Conduite du changement

CA > 20 M€

Près de 200 consultants

- ✓ **Expertises réglementaires et sectorielles** *(Banque/Assurance, Télécom, Transport, Industrie, Santé)*
- ✓ **Certification ISO 27001** sur les prestations d'audits de sécurité
- ✓ Implication forte dans **les organismes professionnels** *(AFNOR, Club 27001, CLUSIF, Forum des Compétences…)*
- ✓ **Convictions et partis pris** *(livres blancs, tribunes, conférences…)*

www.solucominsight.fr

Risk Mgt & Sécurité

De nombreuses approches et solutions pour couvrir de très nombreux risques

Edward Snowden

Rebond

sudo

Break-glass emergency access

APT

Annuaire centralisé

rootkit

Password vault

Mais de quoi parle-t-on ?

Malware

Bastion d'administration

Erreur de déploiement

Collecte de logs

Enregistrement de sessions

Post-mortem

Bombe logique

Durcissement d'OS

Accès tiers

Revue des accès

Révocation d'accès

Comptes à privilèges : 3 risques à maîtriser

- Administrateur système mécontent
- Utilisateur trop curieux

Malveillance interne

Accident

- Erreur de configuration
- Erreur de manipulation lors d'une mise à jour d'un système

Destruction de composants
Vol d'information

Malveillance externe

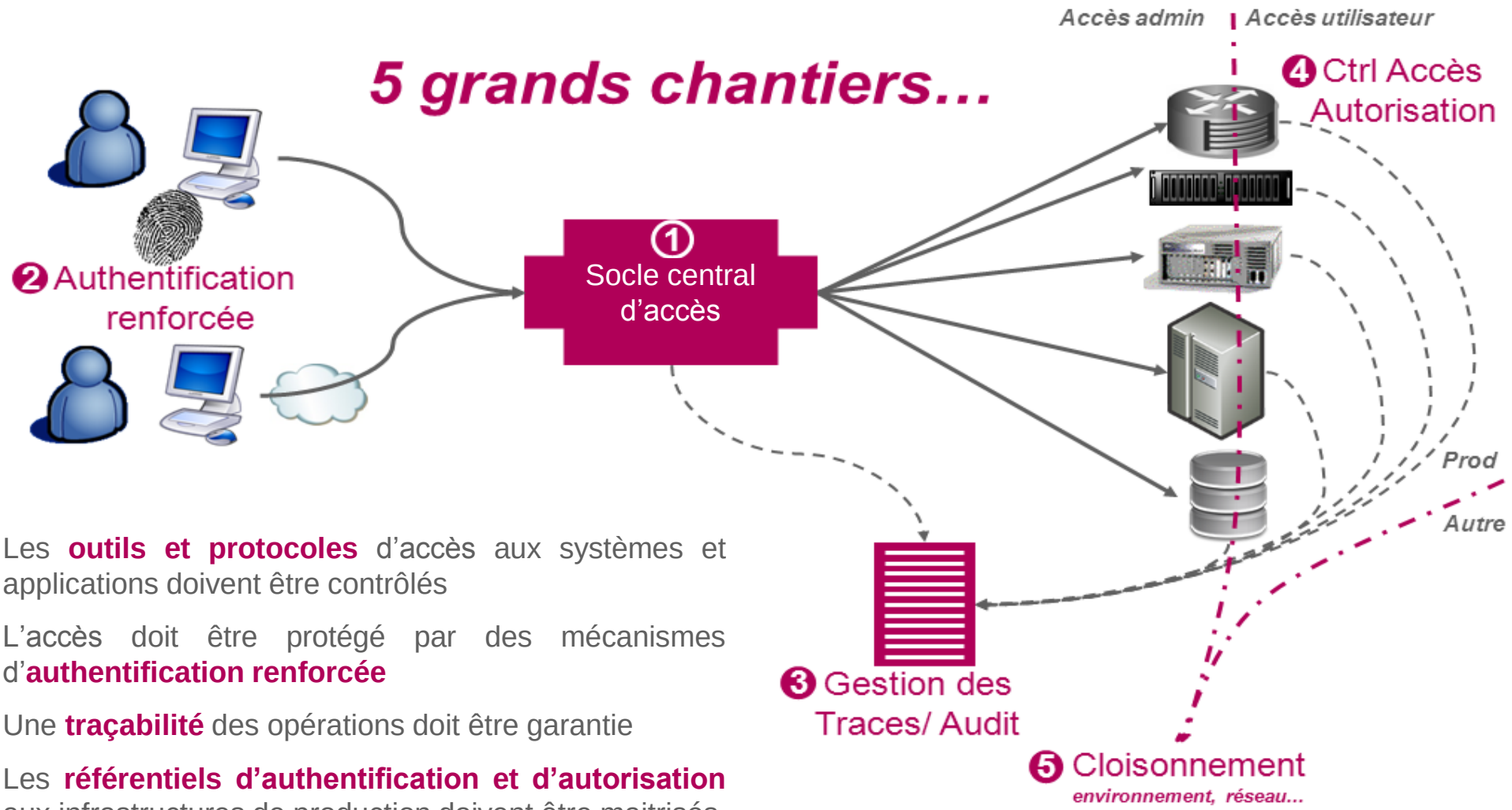
- Exécution de malware dans un contexte à privilèges
- Attaques ciblées sur les administrateurs des systèmes

Prioriser les objectifs…

Habilitations	Audit	Traces
▪ Quels sont les utilisateurs **autorisés à se connecter** sur mes systèmes ?	▪ Quels sont les utilisateurs **qui se sont connectés** sur mes systèmes ?	▪ Quelles sont **les actions effectuées** par les utilisateurs sur mes systèmes ?
▪ Ai-je la maîtrise des habilitations ? ▪ Puis-je révoquer des droits rapidement? ▪ Puis-je retrouver les droits positionnés à un instant t?	▪ Quelle est la fréquence des accès root? ▪ Les processus sont-ils adaptés? ▪ Les habilitations définies sont-elles utiles?	▪ Pour quelles actions root est-il utilisé? ▪ Quelle étape de la procédure a-t-elle été ratée? ▪ Quels documents ont été consultés?

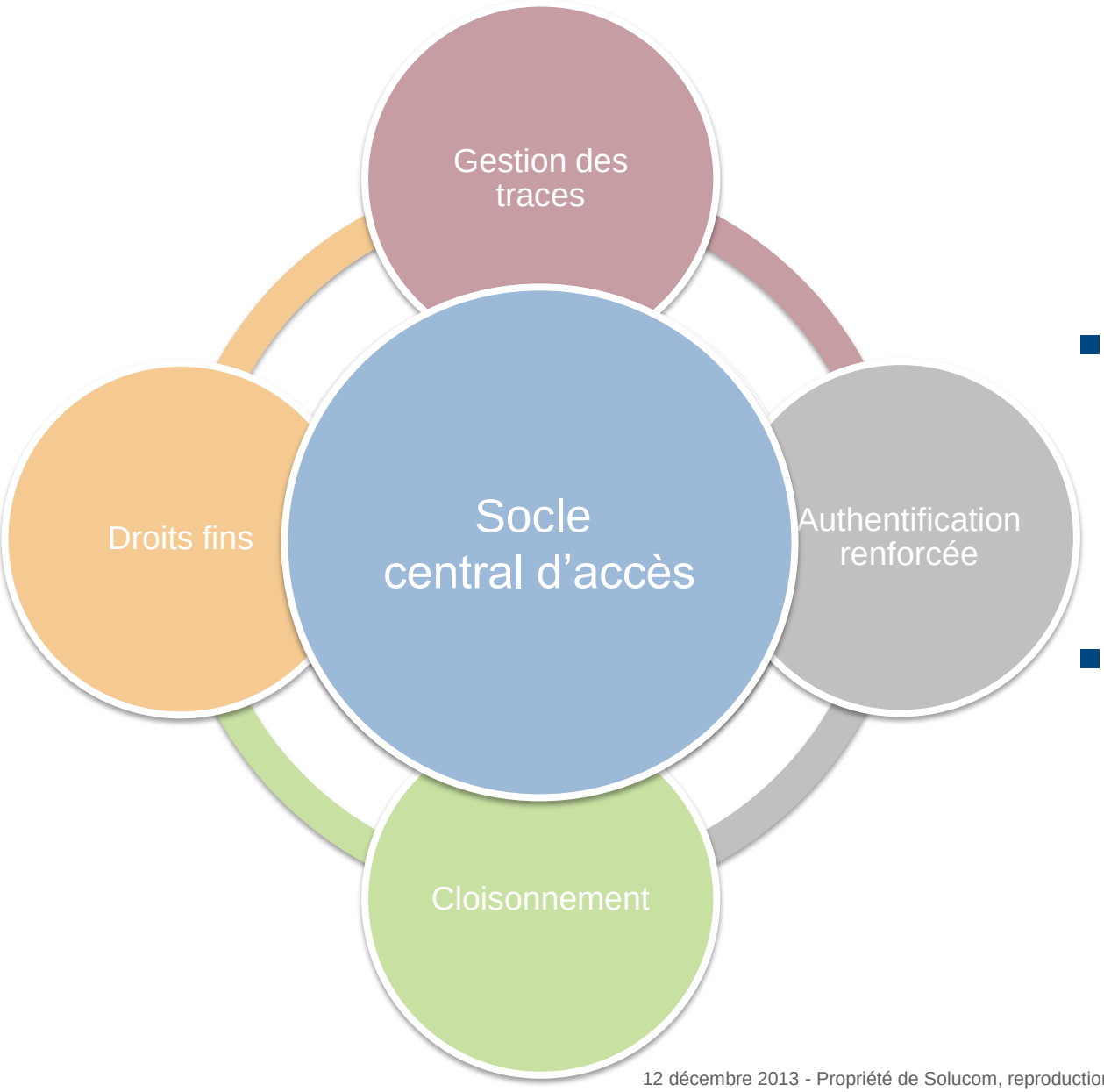
Des solutions complémentaires

Cinq chantiers au service de la gestion des accès privilégiés



1. Les **outils et protocoles** d'accès aux systèmes et applications doivent être contrôlés
2. L'accès doit être protégé par des mécanismes d'**authentification renforcée**
3. Une **traçabilité** des opérations doit être garantie
4. Les **référentiels d'authentification et d'autorisation** aux infrastructures de production doivent être maitrisés
5. Un **cloisonnement** entre production et administration **complète l'utilisation** du socle central d'accès

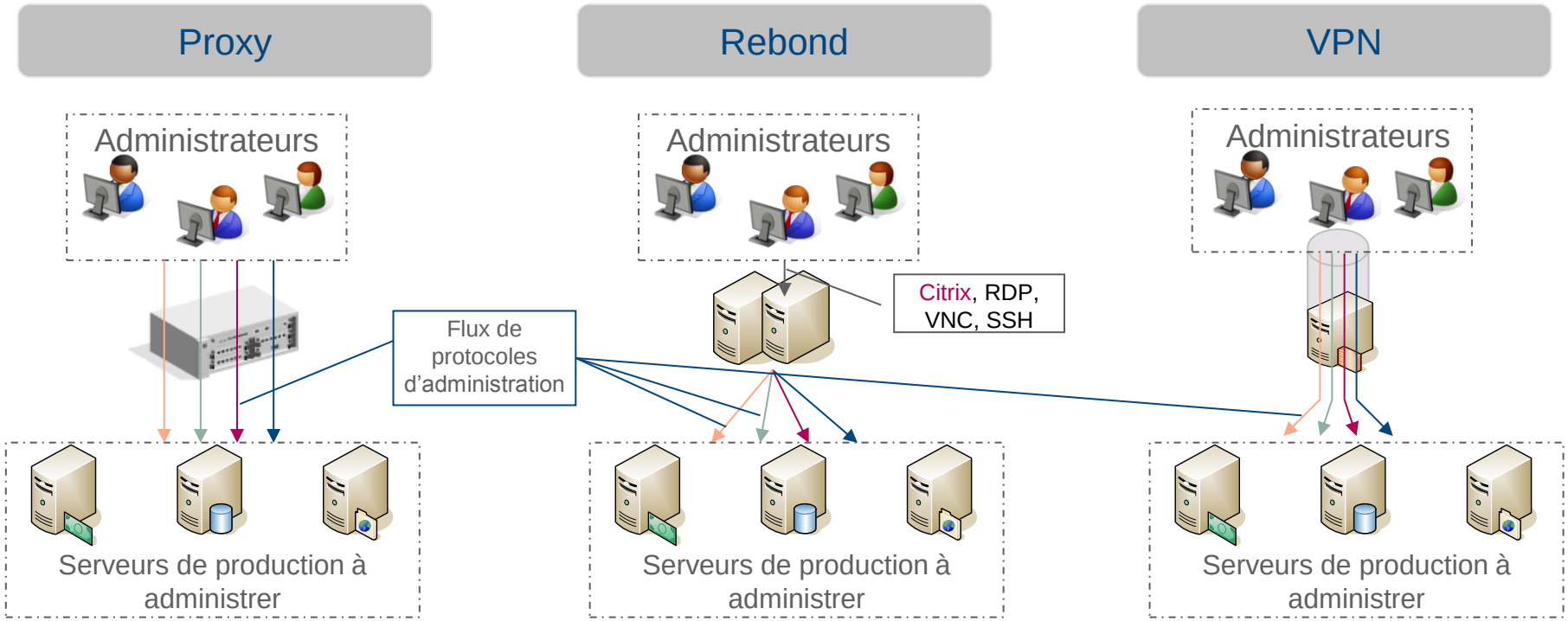
Des solutions complémentaires
Par où commencer?



- Une première brique essentielle
- Un choix de solution structurant

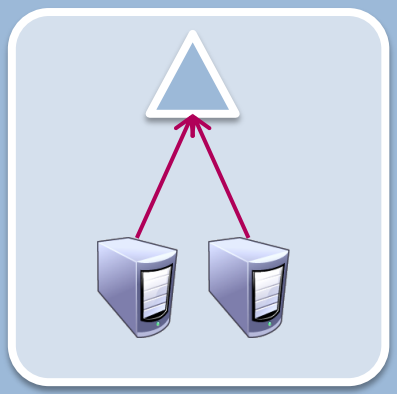
Une tendance notable : le « bastion » d'administration

Un mot qui regroupe plusieurs mécanismes d'accès :



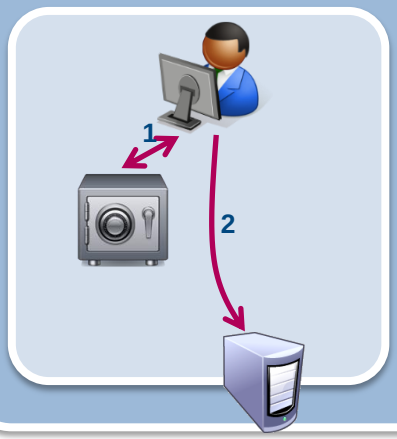
Des impacts sur les protocoles supportés, la finesse de traçabilité, les habitudes des administrateurs, etc.

Les alternatives au bastion



Annuaire centralisé

- Centralisation des comptes & habilitations
- Revue des comptes facilitée
- Coupure des accès en un clic
- Plus ou moins bien supporté par les cibles
- Impose de mettre en œuvre les processus de provisioning

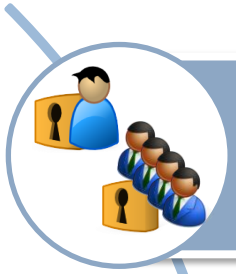


Coffre fort de mot de passe

- Centralisation des habilitations
- Auditabilité des accès
- Accès automatisés (scripts & applications)
- Workflow d'accès, break-glass emergency access

Des solutions complémentaires

À la recherche des meilleures solutions parmi une offre très large



Le contrôle d'accès : du eSSO au coffre-fort de mot de passe

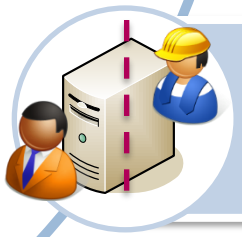
- Différents modes de gestion des mots de passe
- Des solutions spécifiques aux environnements cibles peuvent coexister (e.g. sudo)

Les problématiques de la traçabilité

- En amont : collecte & stockage, standardisation & modélisation
- En aval : alertes, rapports, *post-mortem*, etc.

Authentification renforcée

- Équipements coûteux mais flotte réduite
- Utilisation de la biométrie



Cloisonnement

- Forte réduction de la surface d'attaque
- Nécessité d'une configuration rigoureuse des socles systèmes

L'occasion de se poser les bonnes questions

- De nouveaux outils peuvent amener de nouvelles possibilités
  - « Break-glass » emergency access
  - Délégation d'administration
  - Renouvellement automatique des mots de passe

- Au-delà des comptes d'administration « traditionnels »
  - Comptes d'administration solutions SaaS
  - Administration fonctionnelle des sites institutionnels
  - Identité de l'entreprise sur les réseaux sociaux

twitter facebook Google+

Ne pas oublier…

- Une action essentielle : la charte administrateur

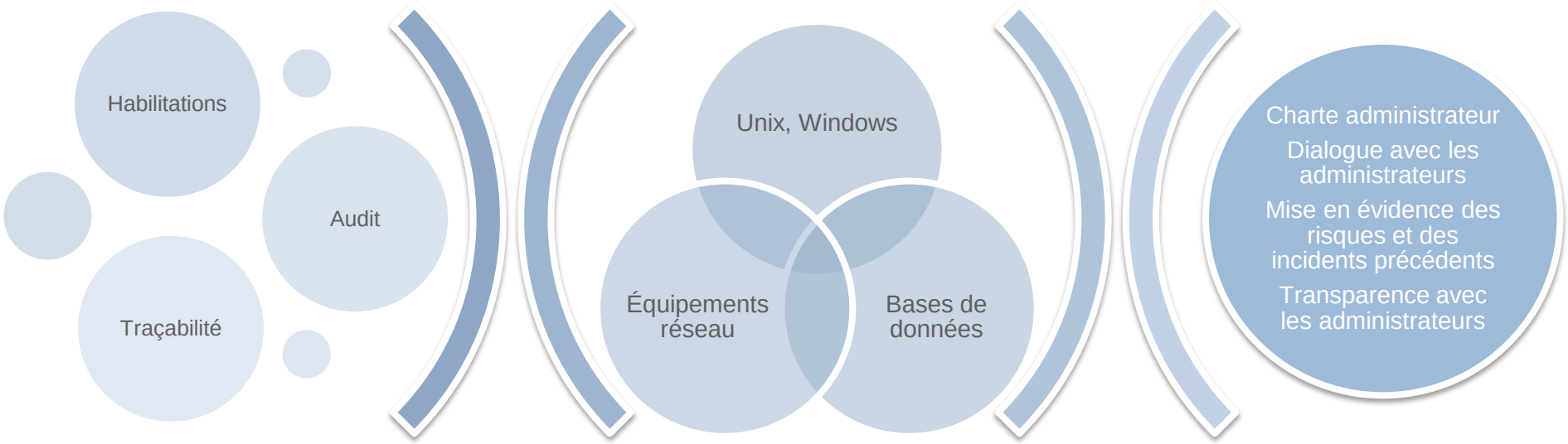
> Pour couvrir quelles populations d'administrateurs ?
> Internes / TMA / Infra / Accès Données…

➔Ne pas négliger l'importance de la conduite du changement

- Dialoguer avec les administrateurs
- Mettre en évidence des risques et des incidents précédents
- Être transparent avec les administrateurs

Les points clés d'une démarche de gestion des comptes à privilèges

Pour se prémunir de quels risques ?
Interne / Externe / Accidentel



Définir les besoins et le niveau de preuve

Définir le périmètre technique

Définir le cadre légal et la conduite du changement

Merci de votre attention !

www.solucom.fr

Contact

Bertrand CARLIER

Manager

Tel : +33 (0)1 49 03 23 12

Mobile : +33 (0)6 18 64 42 52

Mail : bertrand.carlier@solucom.fr