devoteam consulting

Session n°16

Créer un tableau de bord SSI

en 4 fois sans frais

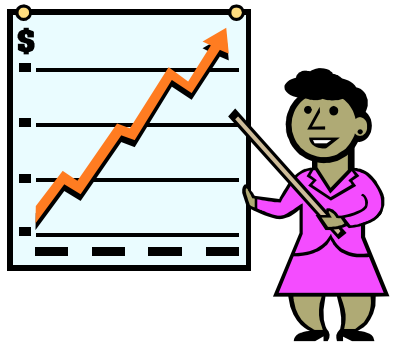
Eric LARCHER
Banque Fédérale des Banques Populaires
http://www.internet-securise.com

Patrick CHAMBET
Bouygues Telecom
http://www.chambet.com

THE EUROPEAN FORUM ON IT SECURITY

FORUM EUROSEC' 2007

Planning

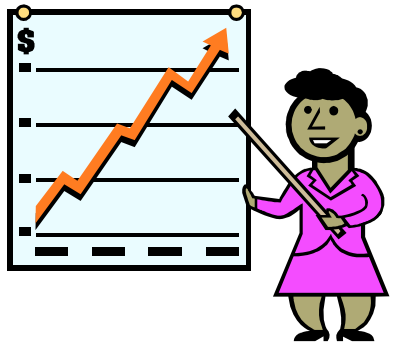


- Introduction
- Étape 1 : Quels objectifs ?
- Étape 2 : Quels indicateurs ?
- Étape 3 : Comment les concevoir ?
- Étape 4 : Comment les restituer ?
- Conclusion

Introduction

- Le tableau de bord de sécurité (TdB)
  - Sujet récurrent, serpent de mer de la SSI
  - Et pourtant meilleur outil de communication interne et de suivi du RSSI
- On peut :
  - Payer (cher !?) un cabinet et/ou un logiciel pour (aider à) concevoir un TdB riche, joli et percutant
  - Mais aussi rapidement mettre en place quelque chose de simple et efficace
    - **à** C'est le but de cette présentation

Planning



- Introduction
- Étape 1 : Quels objectifs ?
- Étape 2 : Quels indicateurs ?
- Étape 3 : Comment les concevoir ?
- Étape 4 : Comment les restituer ?
- Conclusion

1. Quels objectifs ?

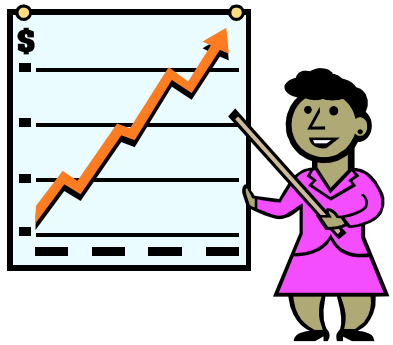
- Que veut-on mesurer ?
  - Le niveau d'exposition / attaques / menaces ?
  - Le niveau de vulnérabilités résiduelles ?
  - Le nombre d'incidents de sécurité identifiés ?
  - L'évolution de la couverture des risques ?
  - Le niveau de déploiement d'une PSSI ?
  - L'état d'avancement des plans d'actions ?
  - Le niveau de conformité aux règlements et autres standards (SOX, PCI DSS, ISO2700x, etc.) ?
- Vers qui veut-on communiquer ?
  - La DG ?
  - La DSI ?
  - Les métiers ?
  - Les corps d'audit et d'inspection ?
- A quelle fréquence ?
  - Hebdomadaire ? Mensuelle ? Trimestrielle ? Annuelle ?

1. Quels objectifs ?

- On distingue trois grandes familles de TdB
  - Stratégique
    - Pour la DG
    - Annuel ou semestriel
    - Suivi de la couverture des risques voire des incidents majeurs
  - De pilotage
    - Pour la DSI / les métiers / l'audit
    - Trimestriel
    - Suivi des plans d'actions, de la mise en conformité
  - Opérationnel
    - Pour la DSI
    - Hebdomadaire à trimestriel (selon les besoins)
    - Niveau d'exposition/attaques, niveau de vulnérabilité, etc.

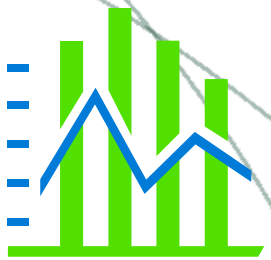
    à Cœur de cette présentation

Planning



- Introduction
- Étape 1 : Quels objectifs ?
- Étape 2 : Quels indicateurs ?
- Étape 3 : Comment les concevoir ?
- Étape 4 : Comment les restituer ?
- Conclusion

2. Quels indicateurs ?



- On peut partir de zéro et faire une séance de… brainstorming !
- Mais il est plus efficace d'utiliser les référentiels existants comme l'ISO17799 (future ISO27002)
  - Il s'agit de définir des grandes familles d'indicateurs, pas forcément d'utiliser les recommandations de l'ISO comme carcan
  - Une fois les familles (domaines et sous-domaines ISO) retenues, identifier deux ou trois indicateurs pertinents par sous-famille
- Ne pas dépasser une trentaine (maximum) d'indicateurs à ce stade de la démarche

devoteam consulting

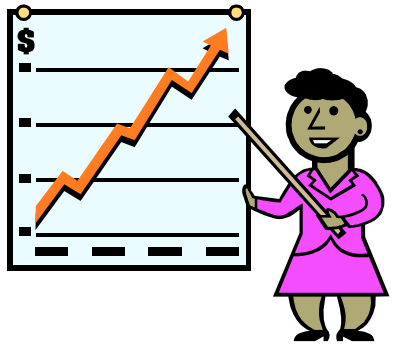
2. Exemples d'indicateurs (1/2)

- % de masters sécurisés disponibles
- % de serveurs conformes, basés sur des masters homologués sécurisés (d'où proportion de machines à migrer, ex: Windows NT 4.0)
- % de postes de travail conformes
- % de postes de travail où l'utilisateur est administrateur local
- % d'antivirus activés et à jour des signatures
- Nb de partage de fichiers avec des permissions d'accès en lecture générale / nb de partages (domaine bureautique / domaine production)
- Nb de documents classifiés confidentiels et stockés non chiffrés
- Nb d'alertes de sécurité traitées par le Service Desk
- Nb d'alertes de sécurité critiques remontées par les IDS
- Nb de vulnérabilités rendues publiques dans le mois
- Nb de correctifs appliqués sur le parc / nb de correctifs diffusés par les éditeurs présents sur le parc
- Nb de vulnérabilités résiduelles sur le parc
- % de projets lancés prenant en compte les normes de sécurité de l'entreprise

2. Exemples d'indicateurs (2/2)

- % d'applications sécurisées (ayant pris en compte les normes de sécurité de l'entreprise) en production
- % de serveurs secourus (reprise sur incident majeur)
- % de serveurs sauvegardés
- % d'équipements critiques redondés
- Nb de comptes génériques / nb de comptes total
- % de mots de passe triviaux pour les comptes génériques
- % de mots de passe triviaux pour les comptes nominatifs
- % de serveurs Unix accessibles en root à distance
- % de serveurs Unix possédant des fichiers .rhosts
- % d'accès prestataires (TMA) sécurisés (authentification individuelle, …)
- % de serveurs configurés par outil de gestion de parc (cf CMDB – ITIL)
- % de couverture de la norme ISO 27001 par la politique de sécurité de l'entreprise
- Etc…

Planning



- Introduction
- Étape 1 : Quels objectifs ?
- Étape 2 : Quels indicateurs ?
- Étape 3 : Comment les concevoir ?
- Étape 4 : Comment les restituer ?
- Conclusion

3. Comment les concevoir ?

- C'est maintenant qu'on redescend vers la terre !
- En effet, un indicateur qui parait extrêmement pertinent « sur le papier » peut se retrouver impossible à générer en réalité
- Il est impératif, pour chaque indicateur retenu de :
  - Définir une formule de calcul précise sur la base d'une ou plusieurs informations à collecter
  - Identifier un mode de collecte (où récupérer l'information et comment ?)
    - Manuel, automatique (quel(s) outil(s) ?)
  - Désigner un responsable
    - Surtout pour les indicateurs techniques, toutes les informations requises ne sont pas forcément disponibles auprès des mêmes équipes
    - Si un indicateur ne peut être généré, on saura qui est le responsable

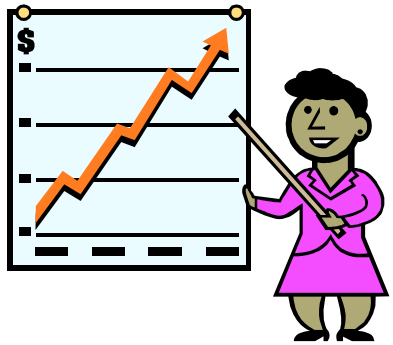
3. Comment les concevoir ?

- C’est maintenant qu’on retouche le sol !
- A ce stade, on s’aperçoit que :
  - Certains indicateurs sont impossibles à obtenir sans lourds développements spécifiques ou même impossibles à calculer « tout court » !
  - Que les outils d’inventaire ou de supervision de peuvent pas donner les bonnes informations
  - Que les responsables… ne veulent être responsables de rien !

3. Comment les concevoir ?

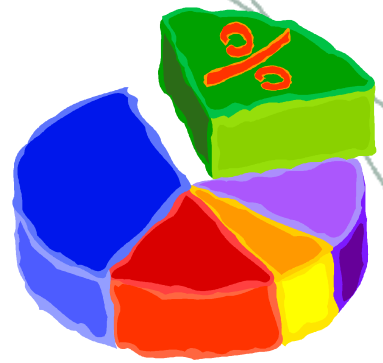
- Avant d'abandonner et d'appeler un cabinet spécialisé à la rescousse, on peut encore :
  - Réduire le nombre d'indicateurs aux seuls vraiment pertinents (30 c'est un peu trop, 15/20 c'est déjà bien)
  - S'appuyer au maximum sur des logiciels ou scripts automatisés (aucun administrateur ne vous donnera de façon pérenne 20 données calculées à la main chaque mois !)
  - Faire le tour des outils « maison » dont on pourrait facilement exploiter le reporting ou définir de nouveaux rapports (scanners de vulnérabilités, IDS, outils d'inventaire, etc.)
  - Faire développer (par un stagiaire ?) des scripts Unix ou Windows pour automatiser la collecte de certaines informations système
  - Se débrouiller tout seul pour certains indicateurs…
- Automatisation et indépendance maximale des autres services = succès !

Planning



- Introduction
- Étape 1 : Quels objectifs ?
- Étape 2 : Quels indicateurs ?
- Étape 3 : Comment les concevoir ?
- Étape 4 : Comment les restituer ?
- Conclusion

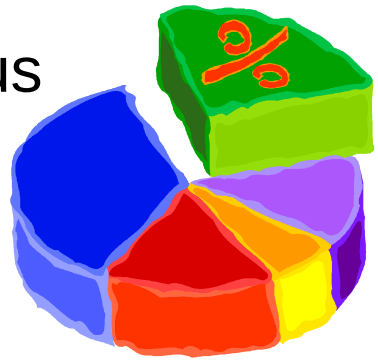
4. Comment les restituer ?



- Le pire reste à faire !
- Un tableau de bord c'est avant tout un… tableau !
  - Il faut « convertir » toutes ces données en représentation pertinente
  - Ne pas négliger cette phase, la forme a autant d'importance que le fond
  - Un indicateur pertinent mais restitué de façon incompréhensible par une majorité de destinataires ne sert à rien
  - Il faut bien réfléchir à la façon dont on va présenter chaque indicateur
    - A-t-on besoin d'une vision historique ?
    - Une capture à un instant t est-elle suffisante ?

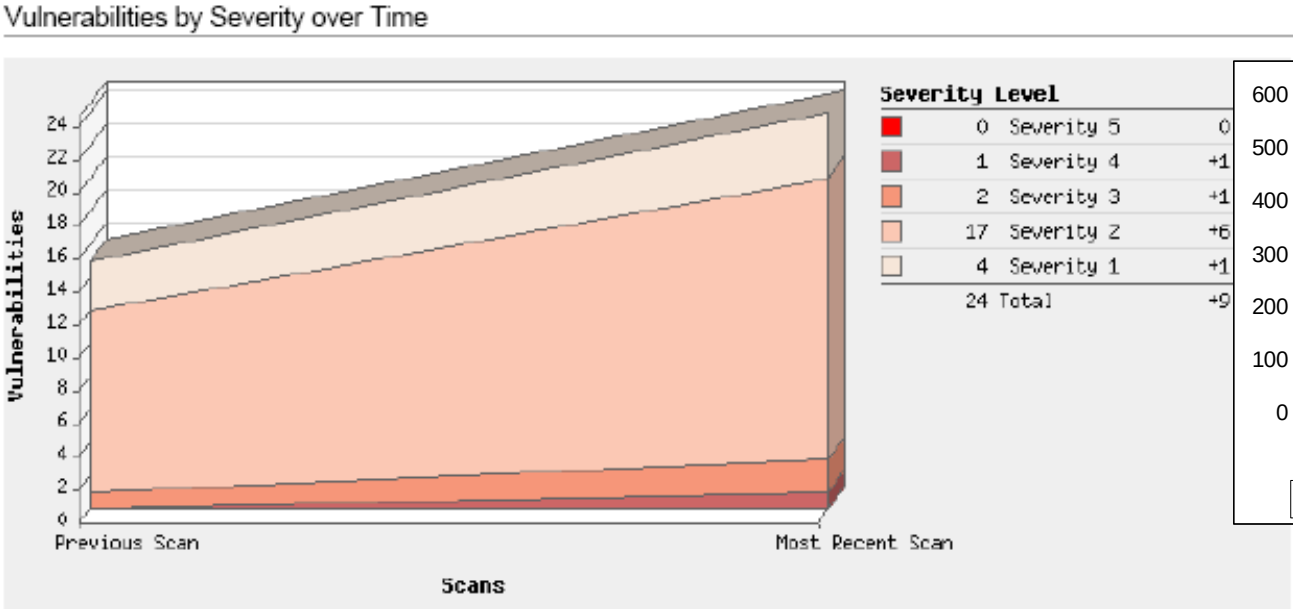
4. Comment les restituer ?

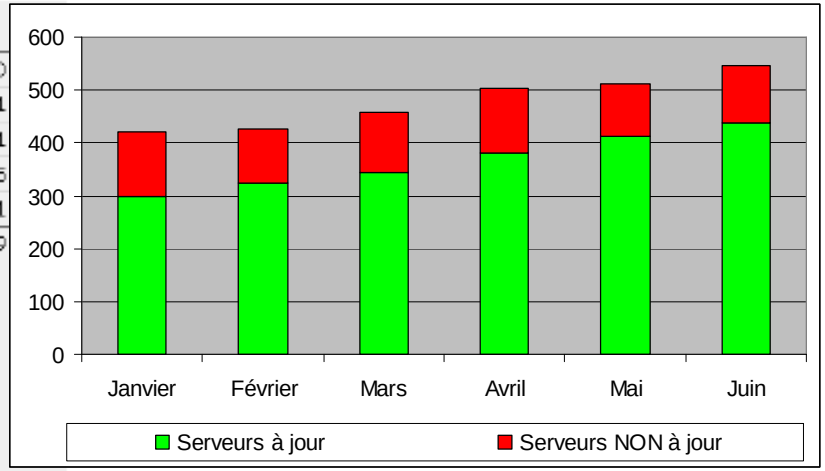
- Y'a-t-il un expert en tableurs dans la salle ?
- Dernière difficulté, la mise en forme
  - Même si vous savez ce que vous voulez, vous devrez maîtriser un minimum le tableur maison avant d'arriver à un résultat pertinent
  - Si vous n'arrivez pas à obtenir le résultat escompté, vous pouvez :
    - Abandonner l'indicateur ou le mode de représentation envisagé (dommage !)
    - Faire plus simple (tant que c'est compréhensible)
    - Rappeler le stagiaire ?



4. Exemples de représentations (1/3)

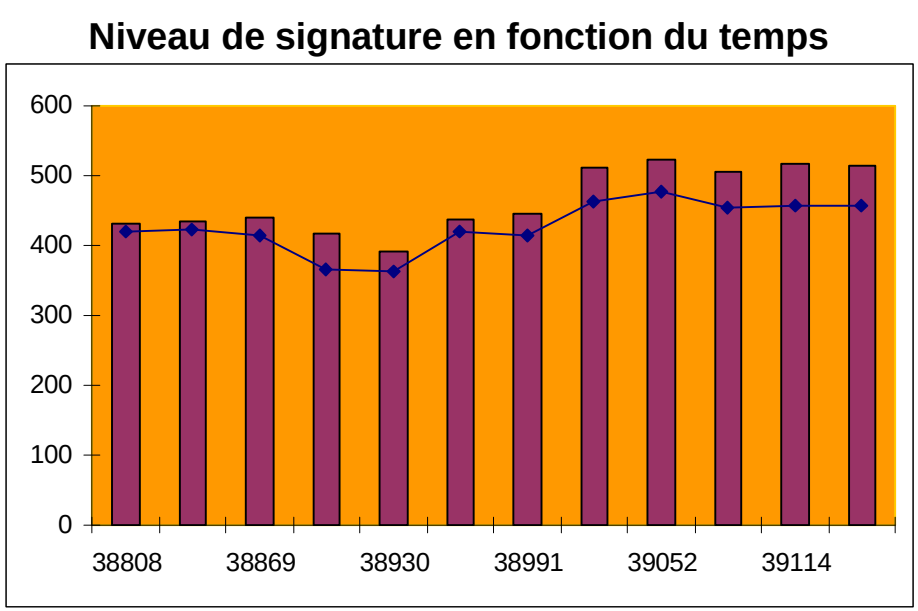
- Vulnérabilités résiduelles sur un parc

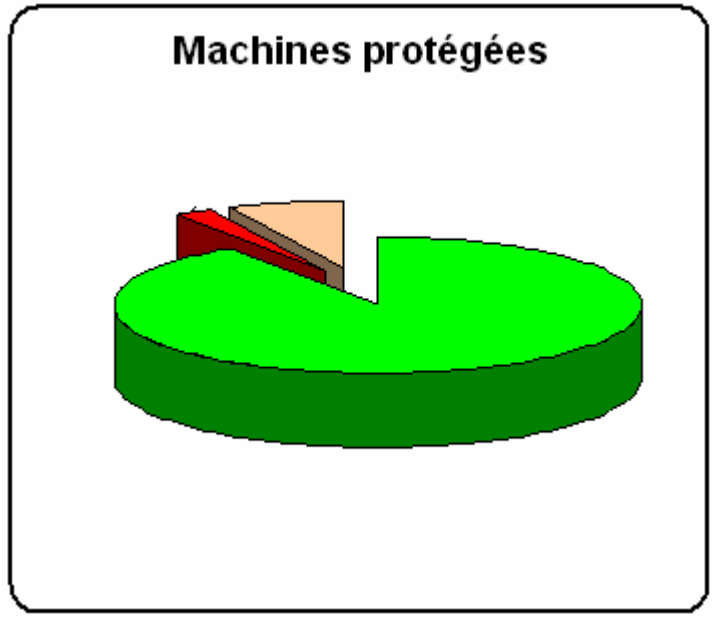




4. Exemples de représentations (2/3)

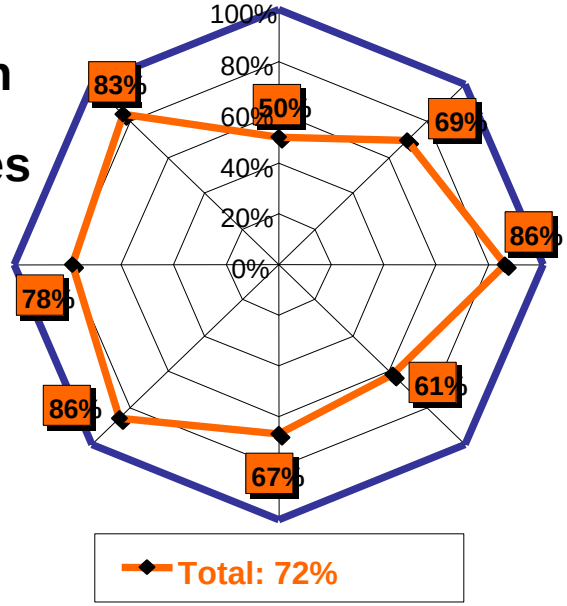
- Protection antivirale

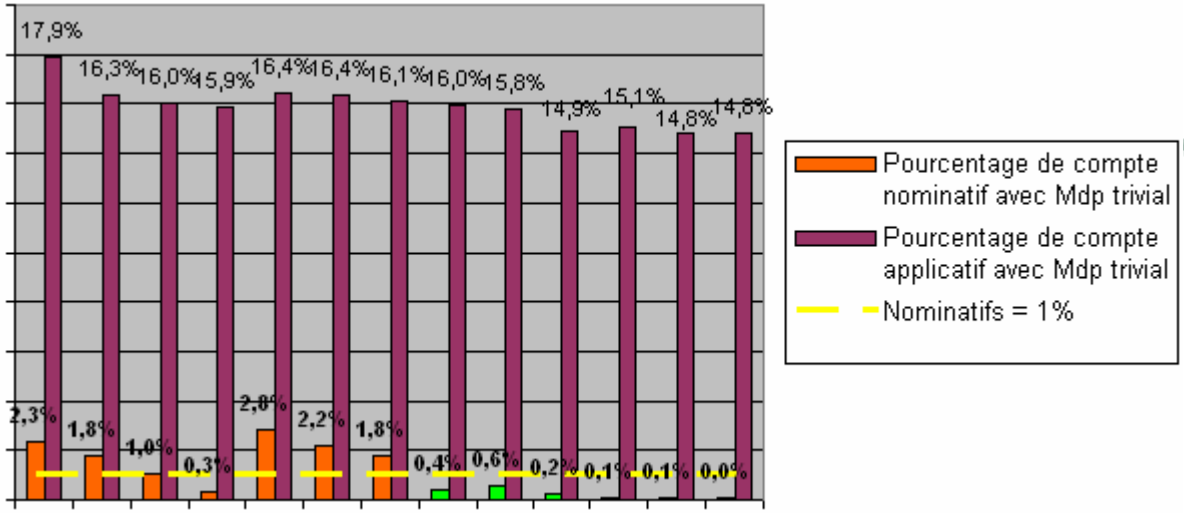


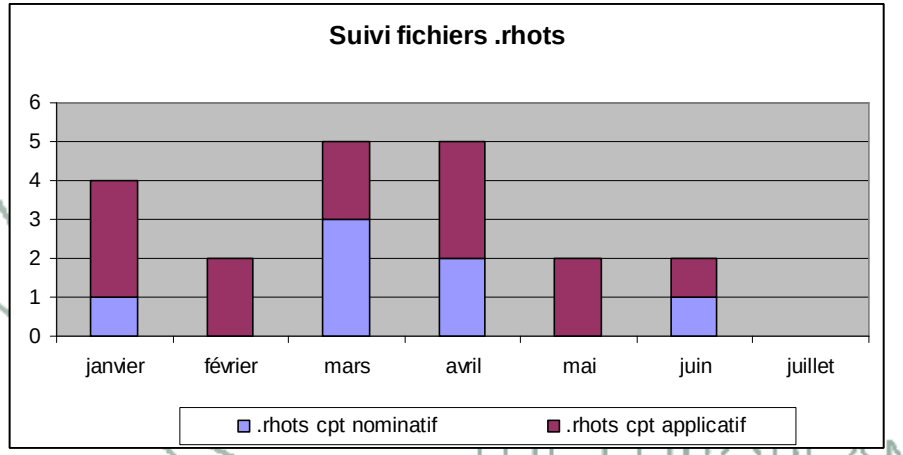


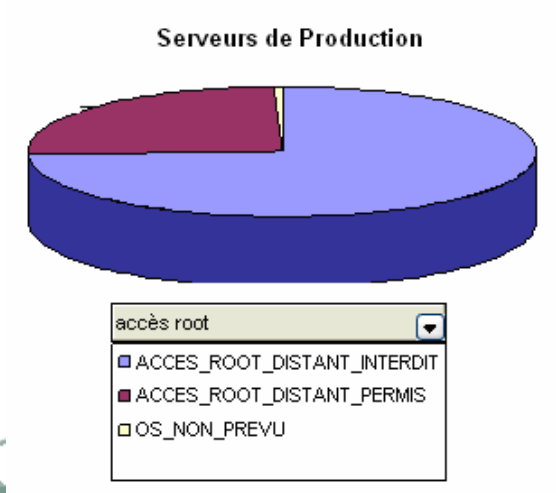
4. Exemples de représentations (3/3)

- **Gestion des comptes**









Conclusion

- Le tableau de bord de sécurité est un instrument de communication privilégié pour le RSSI
- Sa conception nécessite de la réflexion et sa production a un coût, mais le jeu en vaut la chandelle
- En résumé :
  - Se limiter à l'essentiel
  - Automatiser un maximum et ne compter parfois que sur soi-même…
  - Soigner la restitution en faisant simple
  - Etre prudent dans la fréquence de publication (surtout au début)
  - Améliorer au fil du temps les informations remontées et les formats de restitution

Questions