Sécurité des Systèmes d'Information

Tableaux de bord SSI

Nicolas ABRIOUX / Consultant Sécurité / Intrinsec

Nicolas.Abrioux@Intrinsec.com

http://www.intrinsec.com

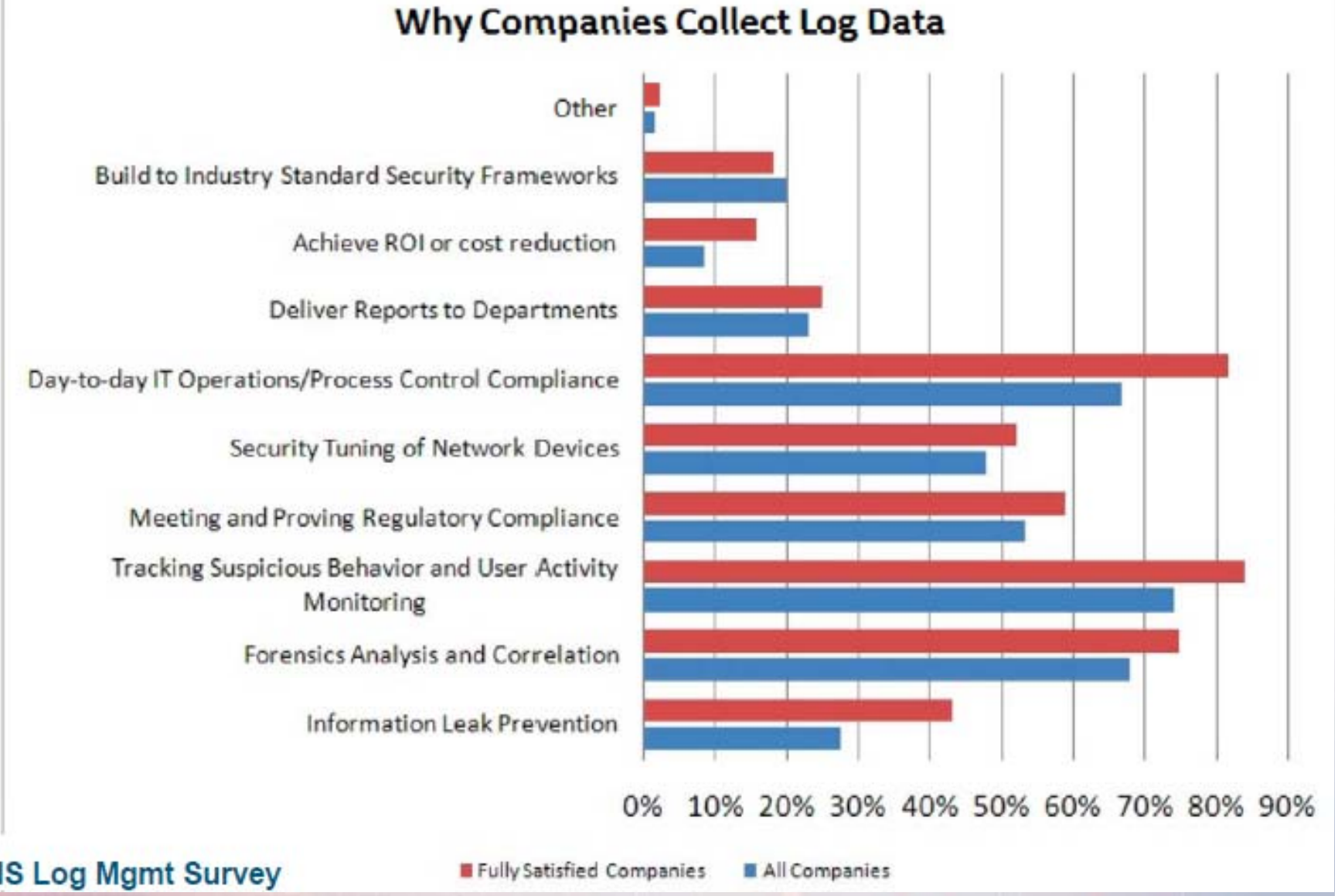
AGENDA

- Pourquoi faire un tableau de bord SSI ?
- Types de tableaux de bord
- Problématiques
- Principe & Vocabulaire
- Méthodologie d'élaboration
- Mise en œuvre
- Points d'attention
- Conclusions

PILOTAGE DE LA SÉCURITÉ & TABLEAUX DE BORD SSI

- Piloter la sécurité de son SI :
  - Identifier ses risques, objectifs de sécurité, mesures de sécurité
  - Appui sur des référentiels internes (PSSI) ou externes (ISO:27002 …)
  - Contrôler son niveau de sécurité, son niveau de conformité
  - Nombreuses vues : technique / organisationnelle, domaines, périmètres…
- Le Tableau de Bord SSI, **un support au pilotage de la SSI**
- Objectifs du tableau de bord sécurité :
  - **Donner de la visibilité** : niveau de risque, conformité (PSSI, réglementations …)
  - **Aider à prendre des décisions** : quelles actions, quelles priorités ? Arbitrages.
  - **Communiquer** : reporting à sa Direction, ses clients ; sensibilisation interne…

POURQUOI COLLECTER DES LOGS ?



DIFFÉRENTS TYPES DE TABLEAUX DE BORD

- Le Tableau de Bord doit être adapté :
  - A ses **destinataires** : RSSI ? Direction ? Clients ? Equipes d'exploitation ?
  - Aux **objectifs et préoccupation** de ceux-ci
    - ➔ *Un outil à personnaliser : pas de « recette » générique*
    - ➔ ***LE** tableau de bord SSI …ou **LES** tableaux de bord SSI ?*

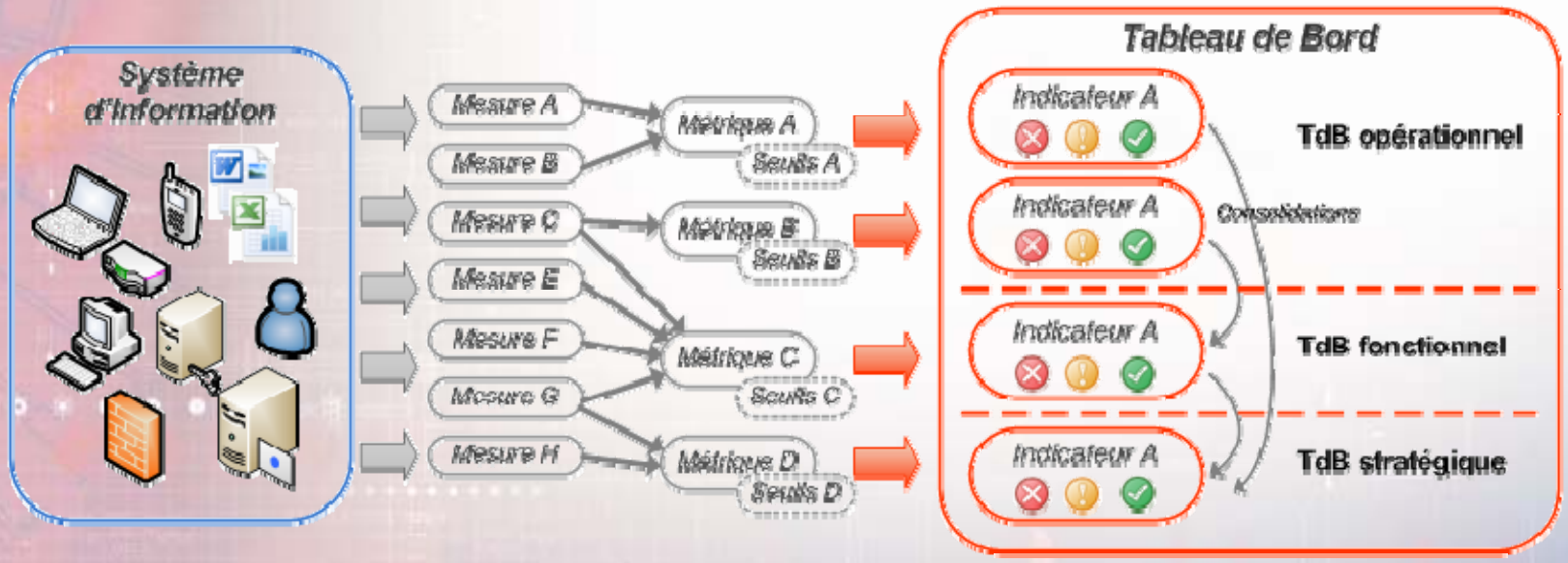
- Tableaux de bord **stratégiques** :
  - Destinataires : Direction Générale, DAF, Risks Managers…
  - Préoccupations : Quels sont les risques ? Vision par activité, branche, site…
- Tableaux de bord **fonctionnels** :
  - Destinataires : RSSI, DSI, Responsables d'activités…
  - Préoccupations : Point de situation par branche / par domaine.
- Tableaux de bord **opérationnels** :
  - Destinataires : RSSI, Equipes opérationnels
  - Préoccupations : Les mesures de sécurité sont-elles appliquées ? Des anomalies ?

PROBLÉMATIQUES

- Un tableau de bord pour aider au pilotage SSI : oui, mais…
  - Nombreuses problématiques :
    - Coût, ressources, outils
    - Pertinence, utilité réelle
    - Maturité SSI
    - ➔ *Approfondissement dans les présentations suivantes !*
- Adopter une construction progressive :
  - **Débuter avec un TdB opérationnel**, portant sur un nombre réduite de thématiques
  - **Elargir progressivement** les thématiques couvertes, au fur de leur maîtrise
  - Accompagner l'évolution de la maturité SSI en s'orientant vers l'approche stratégique
- Finalement :
  - Le manque de maturité SSI n'est pas un frein (TdB opérationnel dans 1er temps)
  - L'intérêt et l'utilité dépendent du choix d'indicateurs pertinents
  - La charge de travail peut être limitée (indicateurs pertinents) et progressive

PRINCIPES & VOCABULAIRE

- **Mesure** = La donnée brute
  - Ex : nombre de postes, criticité d'une vulnérabilité, etc.
- **Métrique** = Fonction de plusieurs mesures (formule de calcul)
  - Ex : la couverture antivirus (nb de postes avec antivirus / nb de postes du parc)
- **Indicateur** = Evaluation d'une métrique en fonction d'un seuil
  - Ex : « CRITICAL », « WARNING », « FEU VERT »…
- **Tableau de Bord** = Présentation synthétique et organisée d'indicateurs



MÉTHODOLOGIES D'ÉLABORATION

- « Top-Down » :
  1. Fixer des objectifs SSI (ou ceux du TdB) ➔ *étape fondamentale (utilité du TdB)*
  2. Déterminer des indicateurs représentatifs, les seuils associés
  3. Identifier les métriques et mesures appropriées
  4. Construction du tableau de bord (calculs, représentation, seuils)
  5. Mise en œuvre (documentations, procédures, fréquence, restitutions)

- « Bottom-up » :
  - Partir des données disponibles pour monter vers les indicateurs
  - Avantage : Certitude de disposer des mesures, de pouvoir les collecter facilement
  - Inconvénient : Risque de sélectionner des indicateurs inutiles / incohérents.

➔ **Ne pas oublier le principal : le tableau de bord doit être un outil d'aide à la décision, en phase avec des objectifs.**

MISE EN ŒUVRE

- Une fréquence dépendante :
  - Des indicateurs (finalité, complexité de collecte)
  - Des décisions prises (laisser le temps d'appliquer les actions, alerter au bon moment)
  - Des destinataires (TdB opé. : quotidien à mensuel, TdB strat. : trimestriel à annuel)
- Approbation du TdB:
  - Les indicateurs ne doivent pas prêter à discussion (nuisible à compréhension / décision)
  - On doit notamment s'assurer de leur pérenité

  ➔ Validation des destinataires et acteurs ; documentation des indicateurs.
- Autour du TdB :
  - Implémentation des mesures (action manuelle, scripts, reportings intégrés, outils…)
  - Procédures et/ ou documentation des indicateurs pour assurer la pérennité du TdB
  - Documentation des indicateurs (sources, fréquence, calcul, seuils…)
  - Modèle de restitution : indicateur + rappel de l'objectif + action / arbitrage requis

POINTS D'ATTENTION

- Restitution :
  - Outil de communication ➔ soigner la présentation, la lisibilité
  - Choix des graphes : peut nuire / aider à l'analyse (ex : représenter les seuils)
- Choix des seuils :
  - Peut être politique (« tout va bien » ou « j'ai besoin de budget ! ») ➔ étape critique
  - Rester réaliste : 100% du parc ne sera jamais 100% à jour…
  - Des objectifs atteignables : doit motiver le travail, pas accabler sous les alertes
  - ➔ Démarrer avec des seuils bas, quitte à les rehausser rapidement après accord commun (élévation du niveau de sécurité)
- Outil de communication :
  - Indicateurs fiables, données cohérentes → attendre plusieurs itérations avant de communiquer

CONCLUSIONS

- Le tableau de bord SSI, un outil précieux :
  - Pour le pilotage SSI
  - Pour communiquer sur sa SSI et échanger entre équipes / branches / directions
  - Pour contrôler sa conformité (PSSI, réglementations…)
  - Peut contribuer à structurer une démarche de gestion de la SSI (PDCA…)
- Sous quelques conditions :
  - Une conception réfléchie
  - Qu'il permette de prendre des décisions, des actions
  - Rester réaliste (objectifs cohérents, ressources nécessaires…)
- Quelques références :
  - Guide ANSSI « Elaboration de tableaux de bord SSI »
  - CLUSIF « Démarche de conception d'un tableau de bord qualité appliqué à la sécurité »
  - CIGREF « Guide méthodologique pour un tableau de bord sécurité opérationnel et stratégique »
  - ≈ ISO:27004 « Information security management – Measurement »