

# Tableaux de bord SSI & Gestion de logs

Vincent Gaillot / Consultant / CONIX







Philippe Vivien-Raguet / Responsable de l'agence lyonnaise / CONIX

vincent.gaillot (at) conix.fr


## AGENDA

- Hit-parade des bonnes raisons de ne pas gérer des logs ?
  - Avantages de l'absence de gestion logs
  - Avantages de gérer trop de logs
- Pourquoi ne pas produire de tableaux de bord ?
  - Avantages de l'absence de tableaux de bord
- Conclusion : risques de se passer de ces 2 outils ?



## Pourquoi ne pas gérer des logs ?

- Absence de gestion de logs :
  - Impossibilité de répondre aux besoins de debug par exemple en cas d'incident majeur ou d'attaque
    - Supervision inutile : les utilisateurs appelleront → gain en fiabilité et efficacité 
    - Gain de temps sur cette étape de debug 
    - Les équipes applicatives ne m'importent plus 
    - Gain de temps général → autre activité ou bien réduction des effectifs
    - Après tout, ce temps est rarement comptabilisé pour l'activité de mon équipe
  - Plus de vision des incidents
    - Absence de logs → tranquillité d'esprit, après tout, je ne trouverai rien. 
    - Aucune corrélation possible → vols d'information silencieux, nuits paisibles 
    - Après tout, si l'entreprise perd ses secrets, puis son business, je n'aurai qu'à en changer 




## Pourquoi ne pas gérer des logs (suite)

- Permet de ne pas respecter certaines normes et bonnes pratiques
  - ISO 27001 SMSI: phase Check du PDCA →
    - pas de confrontation de la sécurité de mon SI à une telle norme → gain de temps
    - plus de besoin de formation à cette norme → gain de temps et argent
  - ISO 27002 best practices: possibilité d'ignorer les contrôles 10.10.n et 15.1.3-4 →
    - Hors la loi (LSF, Bâle, SOX, LCEN et même CNIL) →
      - Métier excitant ++...
      - Par contre auditeurs --
  - ISO 27005 Risk Management : pas de surveillance ni de revue →
    - Mêmes gains que pour 27001
    - Approche pragmatique -- → approche plus poétique de la gestion des risques 
- Allègement de ma PSSI: retrait des paragraphes sur la gestion des logs

J'ai une obligation de gérer les logs (lois...)

- Parade: obligation de moyens, pas de résultats 
- Collecte de tous les logs sans ciblage particulier et sans tuning →
  - Au bout de quelques semaines, volume généré → impossible pour une équipe standard de les gérer → pas de surveillance du tout
- Au pire, choix d'un produit sans faire de PoC sur un petit périmètre → résultats inadaptés à mon organisation ou mes besoins, mais preuve de bonne volonté 

## Je ne produis pas de tableau de bord

- Ignorance des tendances de la sécurité sur mon système d'information →
  - Anticipation impossible → stress lié au mode proactif évité, mode réactif convenable
  - Budget limité suffisant pour sécuriser le peu qui a besoin de l'être
  - Pas de priorité → pile ou face avec le DSI pour déterminer les axes de sécurisation 
- Rien à justifier au DSI ou à d'autres décideurs
  - Même avec des indicateurs fiables et clairs, il peut subsister une incompréhension → gain de temps
  - Heureusement, justification non nécessaire pour l'augmentation de budget ou d'équipe... 
- Non respect des normes existantes: Check du PDCA (27001 et 27005)
  - Aucune confiance dans les groupes de travail internationaux qui ont créé les normes: complot vraisemblable pour faire acheter de la sécurité ... 
  - encore du temps gagné

Je suis quand même forcé de faire un tableau de bord



Je suis quand même forcé de faire un tableau de bord



## Conclusion: Logs et tableaux de bord inadaptés

- Condamné à revivre le passé et répéter les erreurs
- « Errare humanum est, persevare diabolicum »
  - Continuer d'ignorer ce qui se passe dans son SI ...
- Avoir un tableau de bord ne suffit pas : doit être adapté au SI
  - Faire simple ne suffit pas : fonction de la taille du SI et des objectifs fixés par les parties prenantes
- Gestion des logs → relevés bancaires
- Tableau de bord SSI → tableau de bord voiture, train, avion, etc.

Sans gestion des logs ...



Sans tableau de bord...



## Conclusion

- Avoir une gestion des logs même simple et limitée → diminution des risques sur un périmètre limité, connu
- Malgré cela, on peut quand même être victime d'incidents (actualité autant informatique que généraliste)
- Avoir des tableaux de bord adaptés, de bonne qualité et pas trop nombreux → bien piloter la sécurité de son Système d'Informations et mieux communiquer avec les autres parties prenantes
- Globalement, les entreprises survivent quand même

MERCI DE VOTRE ATTENTION

Nicolas Abrioux  
Bernard Foray  
Vincent Gaillot

VOS QUESTIONS SONT LA BIENVENUE