

Tableaux de bord SSI & Gestion de logs

Bernard Foray/ DSSI/ Groupe Casino

bforay@groupe-casino.fr

PROBLÉMATIQUE / OBJECTIFS

- Centralisation de milliers de lignes de logs journalières en provenance des composants sécurité → périmètre + collecte
- Volumes très conséquents
- Formats différents (legacy application) – explication des formats souvent peu documentée
- Dispersion de ces informations sur le réseau
- Stockage et traitement (faut-il faire des sauvegardes des logs, comment garantit-on la confidentialité ?)
- Analyse automatique et qualification en temps réel
- Identification des comportements anormaux (attaques ciblées/généralisées, problèmes de performance, erreurs de configuration, vulnérabilités, etc...)
- Corrélation d'évènements (synchronisation des horloges machines : serveur de temps)
- Investigations et mesure du préjudice causé
- Transmission des résultats de l'analyse (opérateur, mail, sms, déclenchement astreinte, cellule de crise...)
- Niveau de sévérité évoluant en fonction de l'heure des évènements (chgt d'une politique de firewall à 2h du matin...)
- Publication automatique de tableaux de bord

• **....un travail qui ne se voit pas !**

LA RÉALITÉ DU TERRAIN

- Une difficulté de collecte dans une architecture réseau segmentée
- La nécessité de mettre en place des puissances de traitement et de sélection d'évènements au plus près de la source
- Des bases de données à « tuner » régulièrement et qui explosent
- Un flot d'informations inexploitable par un humain
- Un système d'alerte impactant fortement l'organisation humaine
- Ce que prône les vendeurs de solutions != réalité
 - Evolutivité déclaré par les vendeurs d'outils
 - Possibilité de réaliser des requêtes personnalisées (regex ?)
 - Facilité de déploiement et d'intégration
 - Performances
- Sed et awk ont encore de beaux jours devant eux....
- Définir ce que l'on veut auditer

EXEMPLE DE LOGS AUDITÉS

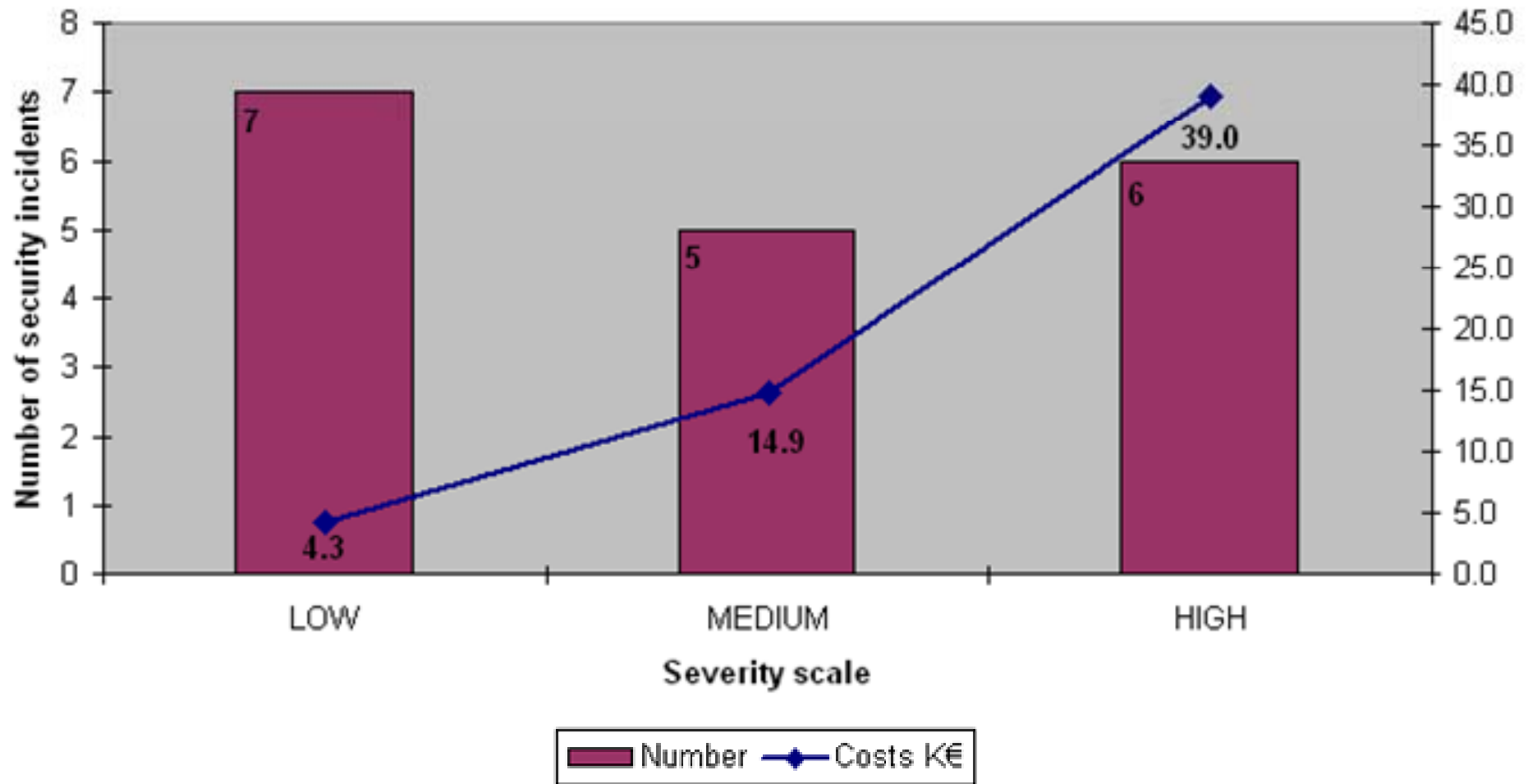
- Systèmes
 - Modification base de compte
 - Tentative de connexions infructueuses
 - Arrêt / redémarrage du système, d'un processus
 - Utilisation de privilèges (root, administrateur)
- Firewalls
 - Ajout, retrait, modification de la politique
- Plate-forme d'administration anti-virus
 - Intégrité des fichiers de signatures
 - Corrélation pour détection de propagation virale
- Proxy
 - Politique de filtrage des url

CE QUE NE FAIT PAS LA GESTION DE LOGS

- Ce n'est pas un IDS
 - Ne surveille pas les flux réseaux ou l'activité système
 - Ne fait pas une analyse comportementale basée sur un référentiel (base de connaissance)
 - Ne génère pas des « False positive »
 - N'est pas une cible potentielle d'attaques
 - Ne dépend pas de l'architecture
 - Respecte la production, ne nécessite pas le déploiement d'agents, les deux outils sont complémentaires
- Ne remplace pas l'expertise humaine
 - Adaptation aux contraintes organisationnelles
 - définition de ce que l'on audite
 - définition des niveaux de criticité et déclenchement de procédures jour/nuit.
 - définition des rapports automatiques
 - définition de la collecte et du stockage de ces informations (respect des flux de données dans la zone démilitarisée)

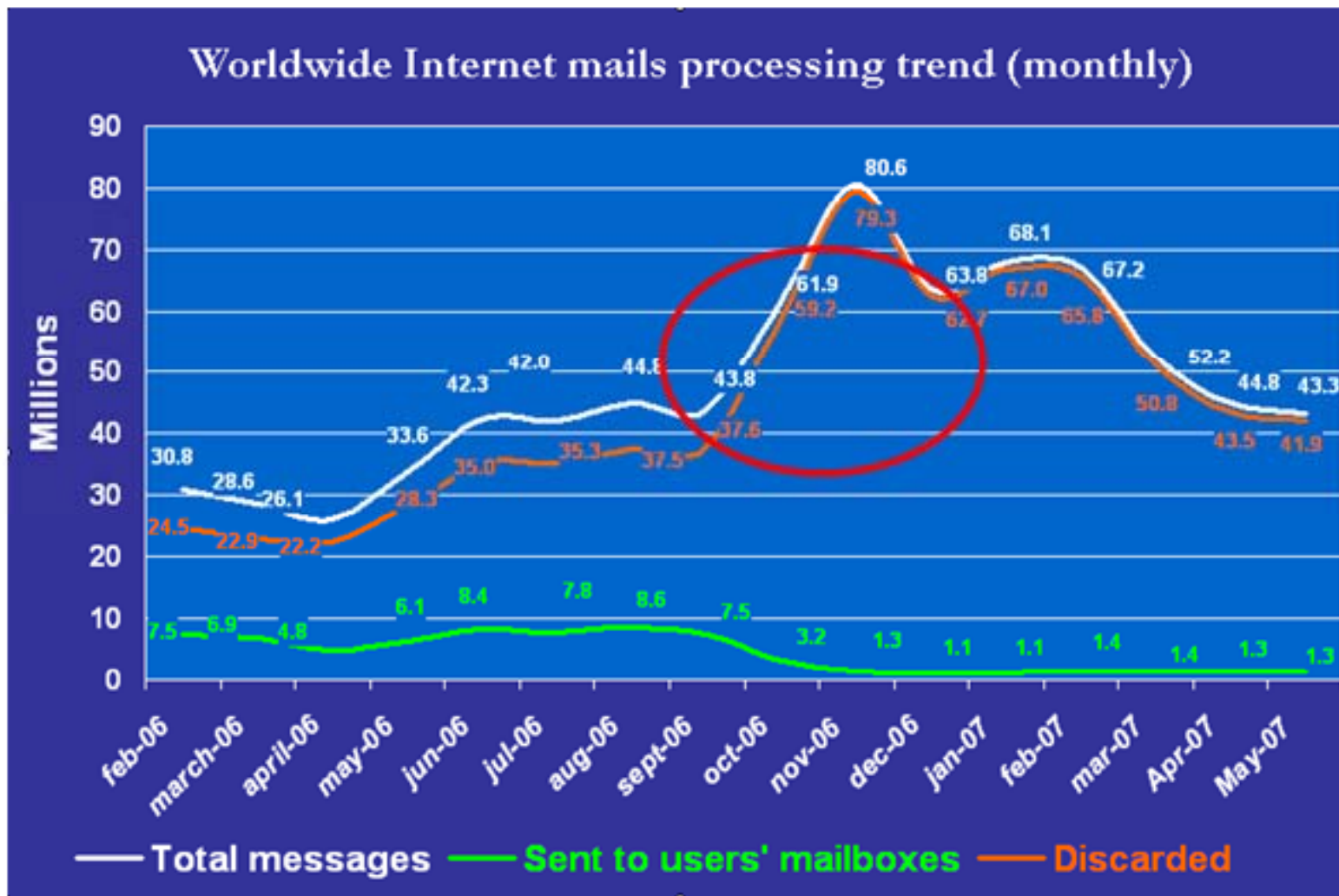
COMMUNICATION/MANAGÉRIAUX

Costs impact of IT security incidents (year 2005)



COMMUNICATION/MANAGÉRIAUX

- Temps de destruction d'un e-mail = 1s
 - $6.000.000 \text{ e-mail} * 1 \text{ s} / 60 / 60 / 8\text{h/j} = 208 \text{ jours de travail/mois}$



COMMUNICATION/MANAGÉRIAUX

Security requests approbation

