

# ***Le facteur humain dans un centre de supervision sécurité***

***Nicolas FISCHBACH***

*Senior Manager, Network Engineering/Security - COLT Telecom*  
nico@securite.org - <http://www.securite.org/nico/>

version 1.0



we make business **straight.forward**



MULTI-PROTOCOL & INTERNET SECURITY CORPORATION

# Agenda

- » Introduction
- » Pourquoi un SOC ?
- » Rôle du SOC
- » Recrutement
- » Gestion du "turnover"
- » Cloisonnement
- » Séparation des responsabilités
- » Outil: SEM (Security Event Management)
- » Risques génériques
- » Conclusion



# ***Pourquoi un SOC ?***

- » **Supervision de la sécurité**
- » **Besoins et obligations**
- » **Multiples sources d'information**
- » **Quantité d'information disponible**
- » **Qualité de l'information disponible**
- » **Centralisation et archivage des informations**
- » **La supervision réseau ou système n'est pas suffisante**
- » **SOC interne ou MSSP pour des clients**
- » **Mutualisation de l'information et des ressources**
- » **Tendance au réactif, peu de proactif**



# ***Rôle du SOC ?***

- » **Supervision sécurité**
- » **Surtout pas d'administration !**
- » **"Change Management" pare-feu, outil de détection d'intrusion/d'anomalie, pot de miel, etc.**
- » **Veille sécurité**
- » **Audits et tests de pénétration**
- » **Analyses post-mortem**
- » **Temps dans le laboratoire ou à "jouer" avec des pots de miel**
- » **Conflit ingénierie/opérations/R&D/etc.**
- » **Perception par les autres départements**



# Recrutement

- » **Quels profils ?**
- » **Compétences/connaissances/attitude**
- » **Qualités: curieux, éthique, parle mieux l'ASM que le français, etc.**
- » **Externalisation/"outsourcing" et où ?**
- » **"Background checking"**
- » **Pas de certification SOC**
- » **Embauches internes et formation à la sécurité ?**
- » **Environnement avec des contraintes fortes**
- » **Privé vs. public vs. militaire/étatique**



# Gestion du "turnover"

- » Comment garder les employés ?
- » 24x7
- » Formation
- » Création d'une base de connaissances interne
- » Beaucoup d'événements peu importants
- » Gestion de l'information et des connaissances acquises: risque de fuite
- » Quels objectifs et quelles métriques pour mesurer l'efficacité ?



# *Cloisonnement*

- » **Besoin de deux réseaux ou plus**
- » **Contraintes de mutualisation**
- » **Protection vis-à-vis de l'Internet**
- » **Risque de contournement**
- » **Remontée d'événements**
- » **Accès pour gestion/maintenance**



# *Séparation des responsabilités*

- » **Administration vs. NOC vs. SOC**
- » **Définir les fonctions: administratif, analyste, veille, etc.**
- » **Risque de copinage (“friends in crime”)**
- » **Problème du manque de connaissances métier (surtout dans les couches hautes)**
- » **“Pipotage” du client (technique et commercial)**
- » **Besoin d’avoir des politiques et des procédures**
- » **Comment trouver un mode de fonctionnement efficace: ressources vs. événements vs. séparation des responsabilités**



# ***Outil: Security Event Management***

- » **Outil de corrélation et de détection d'événements**
- » **Définition des règles**
- » **Information trop/pas assez digérée**
- » **L'interprétation des alertes et anomalies reste très subjective**
- » **Trouver le juste milieu entre ressources et automatisation**
- » **Les erreurs, les mauvaises règles, les informations tronquées se paient: le SOC devient borgne voire aveugle**
- » **Risque de ne pas comprendre ce qui se passe**
- » **Classification des événements: tous les acteurs (hors SOC) n'ont pas la même vision et les mêmes priorités**



# *Risques génériques*

- » **“Who is watching the watchmen”**
- » **Possibilité d’effacer ses propres traces**
- » **Mauvaise adaptation à la couverture attendue**
- » **Gestion de la vie privée et de l’accès aux informations**
- » **Risque que les clients (internes ou externes) se sentent surveillés**
- » **Il vaut mieux ne pas avoir de SOC et en être conscient qu’une “moitié” de SOC...**



# Conclusion

» Conclusion

» Q&R



Image: [www.shawnsclipart.com/funkycomputercrowd.html](http://www.shawnsclipart.com/funkycomputercrowd.html)