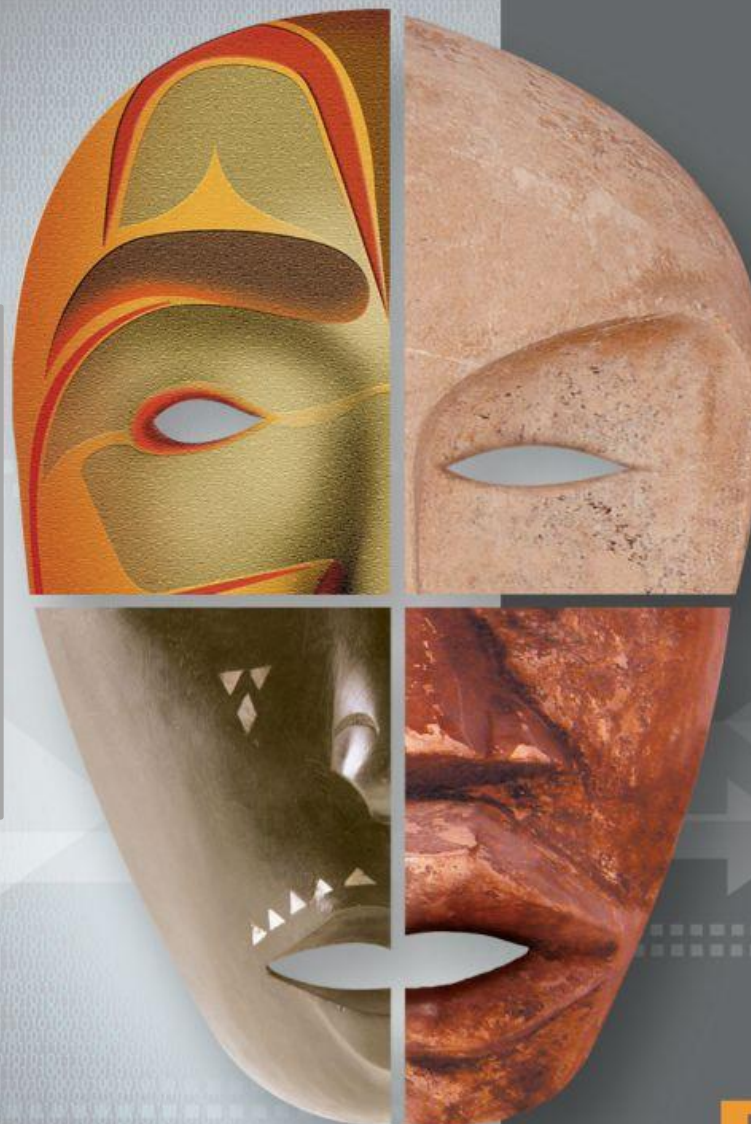


Mardi 17 Mai 2010 à 14h30

« *Des objectifs d'affaires à l'exploitation* »

*Présentation d'un fait vécu :*

- Gestion des risques
- Centre d'exploitation de la sécurité



Conférences  
Expositions

**SECURECOM**  
Services Conseils inc.

**RSI** 2010

Rendez-vous de la **sécurité**  
de l'**information**

## De l'objectif d'affaire à l'exploitation



- Mise en contexte
- Description du cas d'étude (Site e-Commerce transactionnel)
- La gestion de risque ou les besoins d'affaire ?
- Besoins d'affaires et enjeux de conformité
- Facteurs de succès
- Lien vers Michel
- Pause
- Mesures et contrôles dans un contexte d'exploitation
- Cas d'étude
- Service de surveillance des événements de sécurité
- Stratégie
- Défis et Enjeux



# Mise en contexte et déroulement

- Présentation en 2 volets.
  - Accompagnement par l'analyste de sécurité
  - Support de conformité par l'équipe d'exploitation
- La 1<sup>ère</sup> partie couvrira l'approche utilisée pour accompagner l'unité d'affaire dans la réalisation de ses objectifs.
- La 2<sup>ème</sup> partie couvrira les éléments opérationnels permettant de faciliter et consolider les efforts de conformité.
- Conclusion.
- Une seule période de question à la fin de 2<sup>ème</sup> présentation.



# Nos objectifs aujourd'hui

- Trois objectifs
  - Démontrer les avantages d'une étroite collaboration entre la fonction de gestion du risque et les unités d'affaire.
  - Démontrer l'apport positif de la fonction de gestion de risque dans l'atteinte des objectifs d'affaire.
  - (reformuler) Concentré sur l'approche de collaboration avec les lignes d'affaires et non sur la méthodologie et autres outils . (KRI, KPI, etc.)
- (Objectif Michel) Démontrer comment la gestion proactive des événements de sécurité ainsi que la surveillance des éléments critiques contribuent à réduire et à simplifier les efforts de conformité.



# Historique

Début  
2000

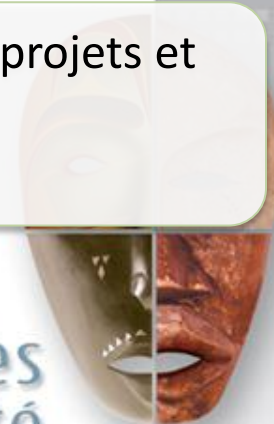
- Surprise! Arrivée des auditeurs: vérification de la conformité.
- Incompréhension, résistance
- Charge de travail supplémentaire

Évolution

- Médiatisation des scandales: sensibilisation, conscientisation
- Formation/appui technique des auditeurs (précision des évidences)
- Augmentation de la charge de travail

Aujourd'hui

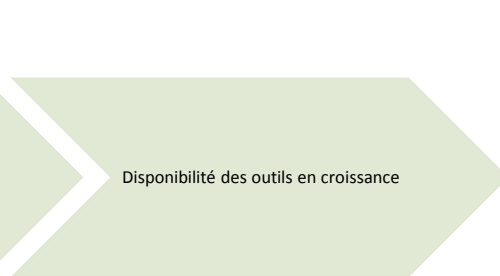
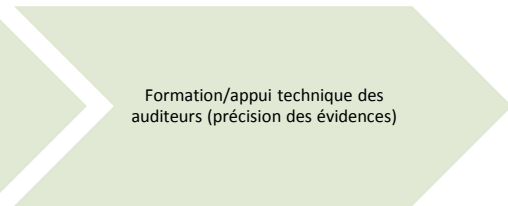
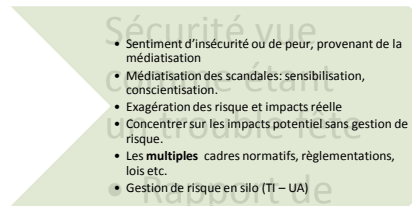
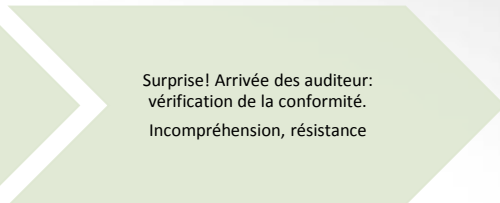
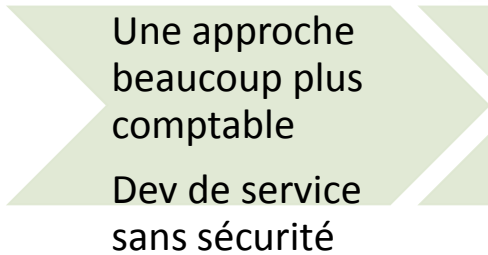
- Nécessité d'intégrer les besoins en conformités dans les projets et les opérations
- Disponibilité des outils en croissance



# Historique et facteurs d'influence

## Analyse et accompagnement

## Exploitation



# Facteurs d'influences (suite)

- Often, technology is acquired to enable a single business initiative without knowledge of the business's entire risk portfolio, risk tolerance, liability, and business goals. As a result, financial and operational resources are poorly allocated, with less important business assets and processes receiving too much investment and those that are more critical receiving too little.
- Mise en marché accéléré.
- Compétitivité.
- Novatrice.
- Avoir désormais une implication auprès des lignes d'affaires permet un repositionnement SI. Non plus limité au déploiement de solution d'appoint mais dans la définition
- Speed to Market, Innovation and Competitive Advantage are what is driving business today. Having a seat at the table with objective and quantitative information shifts the information security focus from deploying reactive to defining strategies that will enable the business securely.



## Défis à relever

- Casser l'image du « Gros méchant loup »
- Parler pour être compris
- Éliminer les frustrations
- Les bons intervenants au bon moment (UA, Architecture, Développement, Exploitation, Gestion risque)
- La sécurité: Un facilitateur, non un fardeau.
- Le facteur humain 😊
- Collaboration ouverte

- Mettre les points de Michel et Éric provenant de la slide transition



# Transition

- Communication et compréhension des besoins d'affaires
  - Enjeux et conformité
- Intégration des besoins de mesures et contrôles très tôt dans le cycle de développement de nouveaux services
  - Levier pour les besoins d'exploitation
  - Identifier et gérer les impacts: temps / ressources / budget
  - Permet d'automatiser les besoins et réduire les impacts opérationnels
  - À considérer à l'intérieur de tous les projets
- Investir le temps nécessaire lors de la mise en place initiale (mettre les bases) afin d'optimiser le suivi récurrent



# Besoins d'affaires vs Sécurité

## Besoins d'affaires

1. Nouveau service avec paiement en ligne.
2. Sauvegarde de données sensible clients.
3. Assurer une haute disponibilité du service.

## Requis de sécurité/Conformité

1. Conformité PCI, SOX, etc., intégrité des données, non-répudiation.
2. Conformité PIPEDA, etc. confidentialité des données.
3. Redondance et surveillance



## Facteurs de succès

- **Rephraser les énoncés plus bas de façon à faire ressortir les éléments positifs et comment ils peuvent influencer les décisions et permettre d'éviter certains pièges.**
- Often, technology is acquired to enable a single business initiative without knowledge of the business's entire risk portfolio, risk tolerance, liability, and business goals. As a result, financial and operational resources are poorly allocated, with less important business assets and processes receiving too much investment and those that are more critical receiving too little.

Speed to Market, Innovation and Competitive Advantage are what is driving business today. Having a seat at the table with objective and quantitative information shifts the information security focus from deploying reactive point products to defining strategies that will enable the business strategically and securely.

Technologists must integrate a new language into their vocabulary to communicate complete, clear, unbiased and useful information about threats and available mitigations.

- Permis d'éviter le piège



# Approche (1 de 2)

- Au-delà des méthodologies d'analyse de risque.
- Modifié le vocabulaire et discours TI
- Participé tôt et activement dans l'initiative d'affaire.
- Accompagné l'UA dès le début.
- Participation active de l'équipe d'exploitation .
- Analyse transversal.



# Approche (1 de 2)

- Au-delà des méthodologies d'analyse de risque.

GOUVERNANCE ET GESTION DE LA SÉCURITÉ

RELÈVE ET CONTINUITÉ DES OPÉRATIONS

Unité d'affaire

Sécurité  
applicative

Sécurité des  
infrastructures

Sécurité de  
l'exploitation

Vérification et  
conformité

- Analyse transversal.



## Approche (2 de 2)

- Identifier à haut niveau les enjeux et les répercussions potentiels.
- Définir la stratégie et les options possible
- Refaire une session de travail avec l'UA pour discuter des avenues possible

(De là, nous avons commencer à nous greffer d'avantage à ce qui pourrait ressembler à de la « gestion de risque d'entreprise »



# Bénéfice de l'approche

Permettant d'identifier rapidement et concrètement les exigences  
légal, réglementaire et autres;

Désamorcer les tensions;

Lorsque utilisé ainsi démontre une grande valeur pour l'entreprise en :

Augmentant la compréhension de tous les intervenants;

Ce que cette approche a permis de faire:

Time to market plus rapide

Augmenté la communication.

Diminué la frustration due à l'incompréhension ou la perception  
d'incompréhension

- Le conseiller a joué un rôle déterminant dans l'atteinte des objectifs de l'entreprise par sa collaboration et son apport en tant que facilitateur entre la fonction TI et l'UA



## En résumé

- En résumé, ce qui nous a mené à cette approche c'est tout simplement d'avoir été à l'écoute des gens.
- Si les gens au dev ne sont pas content;
- Si les gens en exploit ne sont pas content;
- Si les architectes ne sont pas content;
- et si les gens d'affaire ne sont pas content.
- Y doit y avoir quelques chose qu'on fait de pas correcte!
- C'est certain, on peut toujours se dire, Ah, c'est parce-qu'ils sont contre la sécurité. Mais, les gens ne son pas contre la sécurité. Ils sont contre se faire imposer des choses et se faire dire quoi faire sans en comprendre le pourquoi.



# Liens vers l'exploitation

Décrire brièvement le lien vers l'exploitation



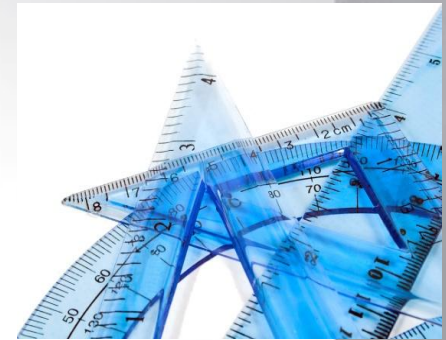
# Exigences et contrôles

- À définir clairement (liste des exigences, contrôles)
- Reprendre la liste



## Moyens

- Gestion intégrée et centralisée des journaux
  - Infrastructures, Services de sécurité, Applications
  - Activation et analyse du contenu
- Surveillance des évènements
  - Détection d'évènements identifiant des comportements inappropriés ou malicieux
  - Analyse
  - Recommandations et actions

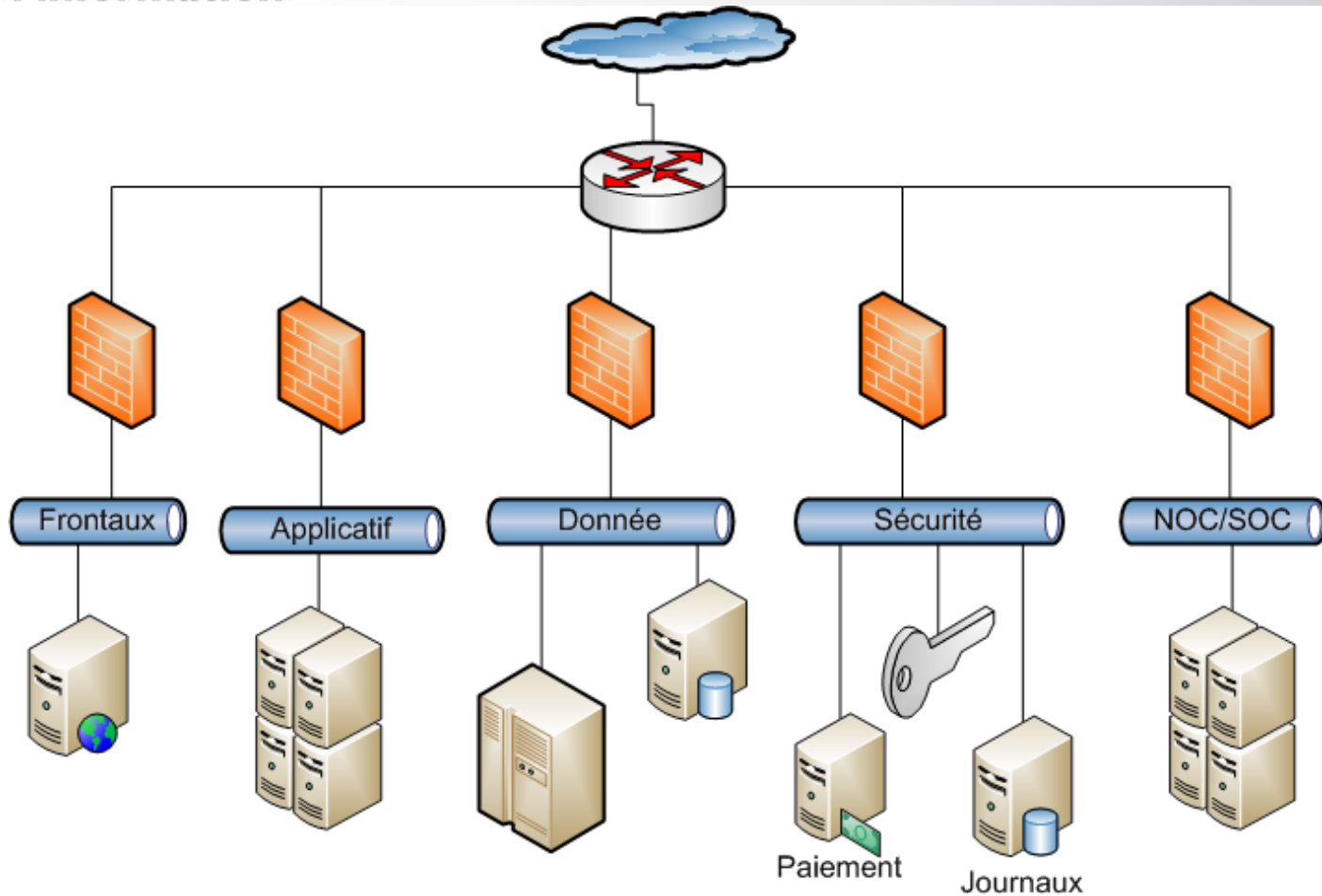


# Cas d'étude

- Schéma système (appl., serveurs, réseau, composants) Éric....
- Volumétrie
- (à schématiser)



# Cas d'étude: Web Transactionnel

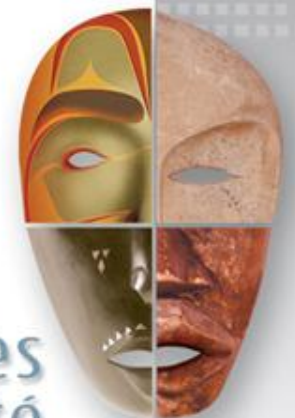


- Service de surveillance des événements de sécurité
  - Objectif : Contribuer à l'atteinte des objectifs d'affaires en assurant le maintien des services (disponibilité, intégrité, confidentialité)
  - Pourquoi un Centre de surveillance



les **visages**  
de la **sécurité**

Au-delà des apparences



# Service de surveillance

(Schéma Éliot)



les **visages**  
de la **sécurité**

Au-delà des apparences

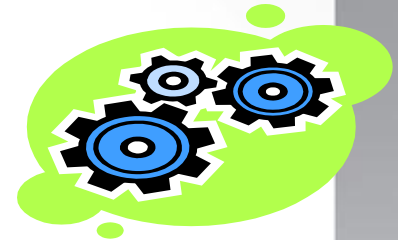
# Besoins opérationnels

- Cas de surveillance
- Sources de journalisation
- Information sur les actifs
  - Technologies
  - Versions
  - Configuration
  - Paramétrage
- Outils: optimisation, automatismes
- Processus et procédures
- Ressources formées et compétentes
- Fournir des évidences



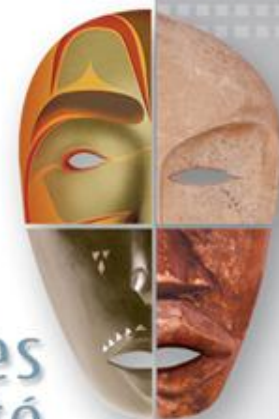
# Composition du service

- Processus et procédures
  - Garantie la cohérence et récurrence
- Équipe
  - Organisation de la surveillance en temps réel et différé
  - Formation (technologies et bonnes pratiques en sécurité)
  - Rôles et responsabilités
- Outils
  - Solution de journalisation
  - Engin de corrélation: Alertes, règles, tableau de bord, rapports
  - Base d'actifs (CMDB) et billetterie
  - Base de connaissances
  - Documentation
  - Balayage de vulnérabilités et détection d'intrusion



## Bénéfices

- Vues centralisés des évènements de sécurité
- Répond aux exigences de conformité
- Broken windows theory
- Optimisation de l'utilisation des TI:
  - bande passante
  - Correction erreurs configurations (ex : SNMP public, mauvaises routes) ;
- **Démontrer pourquoi un événement de basse sévérité doit aussi être traité et appui aussi la gestion de risques**
- **Plus grande flexibilité**
- **Proactif au lieu de réactif**
- **Cheminement naturel vers la GRE**
- **Solution intégré**
- **Conscientisation et sensibilisation à tous les niveaux**



# Stratégie de mise en place

- Étapes et méthodologie
  - Définir la cible
  - Procéder à la mise en place par étapes
- Défis et enjeux
  - 24/7 à tout prix?
  - Recherche vs volume (charge de travail)
  - Disponibilité des sources de journalisation
  - Impacts dans l'organisation (autres équipes)
  - Gestion du changement
  - Gestion des RH
    - Embauche
    - Maintien des connaissances (roulement de personnel / motivation)



# Communications

- Tableau de bord (suivi)



# Conclusion

- Gestion de risque d'entreprise au lieu de simplement TI

