

BeH



Séminaire sur les solutions de sécurité

Savoir maintenant pour agir rapidement

André Beaudoin

2009-11-12

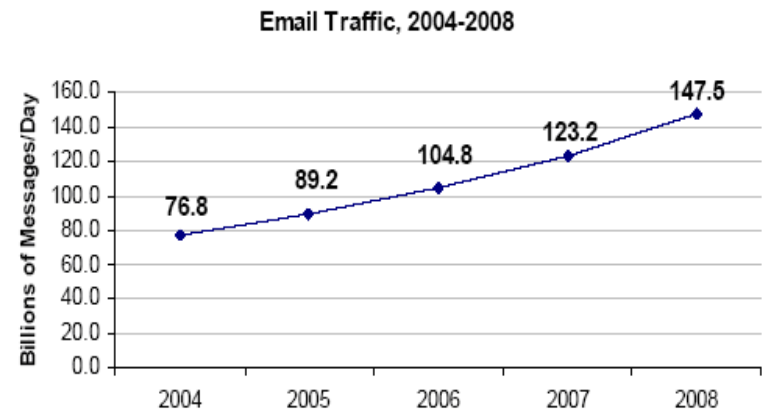
Bell



Contexte

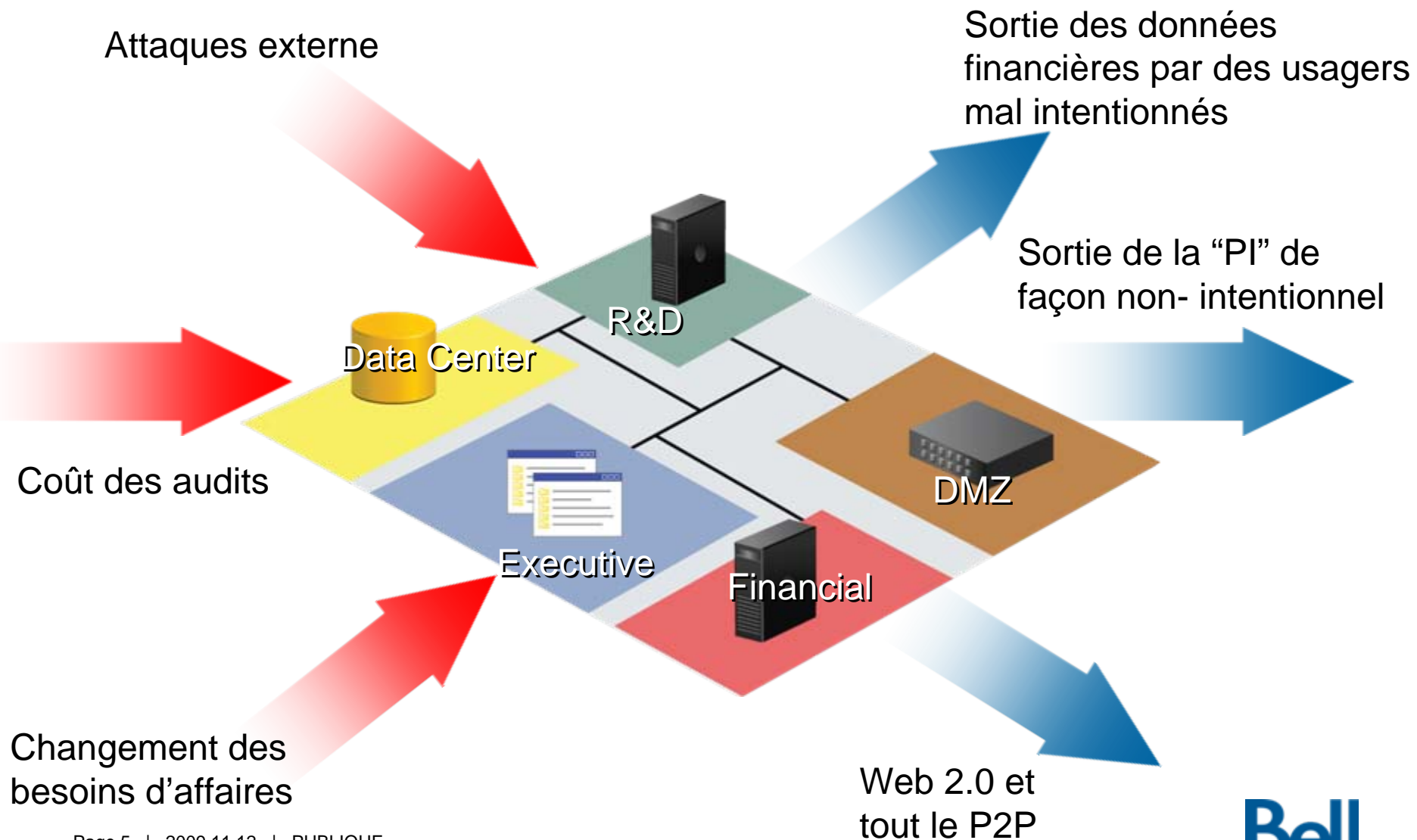
Une époque de défis:

- Les réseaux informatiques des entreprises sont constamment assiégés par des pirates et des attaques internes malveillantes, prêts à exploiter chaque vulnérabilité;
- Le nombre d'attaques sur les systèmes n'a cessé de croître de manière exponentielle



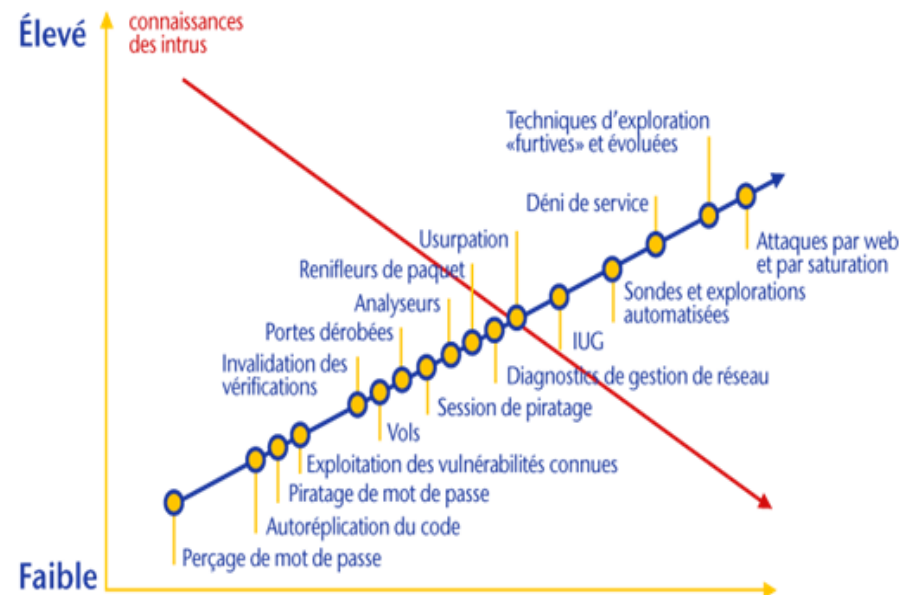
En 1988, le Centre de Coordination du CERT n'a enregistré que six attaques contre les systèmes connectés à Internet. En 2005, ce chiffre est monté en flèche pour atteindre environ 200 000 attaques.

Contexte (suite)



Contexte (suite)

- Ces attaques n'augmentent pas seulement en terme de fréquence, mais également en terme de complexité et de gravité;
- La nouvelle réalité est aussi que la durée d'exploitation des vers et des virus les plus sophistiqués actuellement est passée de quelques années à quelques mois puis à quelques jours, voire, parfois, quelques heures.



Les défis

Cet état de choses oblige les organisations à prendre action:

- Les besoins d'affaires:
 - Protection de la marque – confiance des clients;
 - Interaction avec les différents partenaires – réseau ouvert et étendu;
 - Protection de la propriété intellectuelle – protection de la valeur
- Les obligations légales:
 - La conformité financière – Sarbannes & Oxley, C-198
 - Les cartes de crédit – Standard PCI (Payment Card Industry)
 - Protection des renseignements personnels – PIPEDA

Les défis (suite) Obligations

Les Amériques

SOX (US)
HIPPA (US)
GLBA (US)
USA Patriot Act (US)
Tax Act (US)
NASD rules (US)
FDA 21 CFR 11 (US)
SEC Rule 17a-3 & 17a-4 (US)
CAN-SPAM Act (US)
FTC Do-Not-Call List (US)
COPPA (US)
NIIPA (US)
SB 1386 (California)
PIPEDA (Canada)
FATF (Latin America)

International

Basel II
Information Security Forum
OECD guidelines
ISO

Europe

LSF (France)
KonTraG (Germany)
BDSG (Germany)
SigG (Germany)
RIP (UK)
Tumbull Report (UK)
HRA and DPA (UK)
NERC (Ukraine)

EU Convention of Human Rights
EU Privacy Directive
EU Signature Directive
WEE Directive
RoHS Directive
Antitrust Rule

Asie

Protection for Personal Information Act
JSOX

Afrique du Sud

King II Report

Australie

Federal Privacy Act
Privacy Amendment Act
Spam Bill
PSM
ACSI 33

Les défis (suite)

- Les organisations ont essayé de se protéger en mettant en œuvre des solutions de sécurité à la pointe de la technologie comme des passerelles antivirus, des pare-feu et des systèmes anti-intrusion. Ces technologies sont très précieuses, mais elles ont été la source d'un nouveau problème :

Une complexité handicapante

Les défis (suite)

D'avoir la capacité de recevoir un événement en temps réel et de prendre action immédiatement

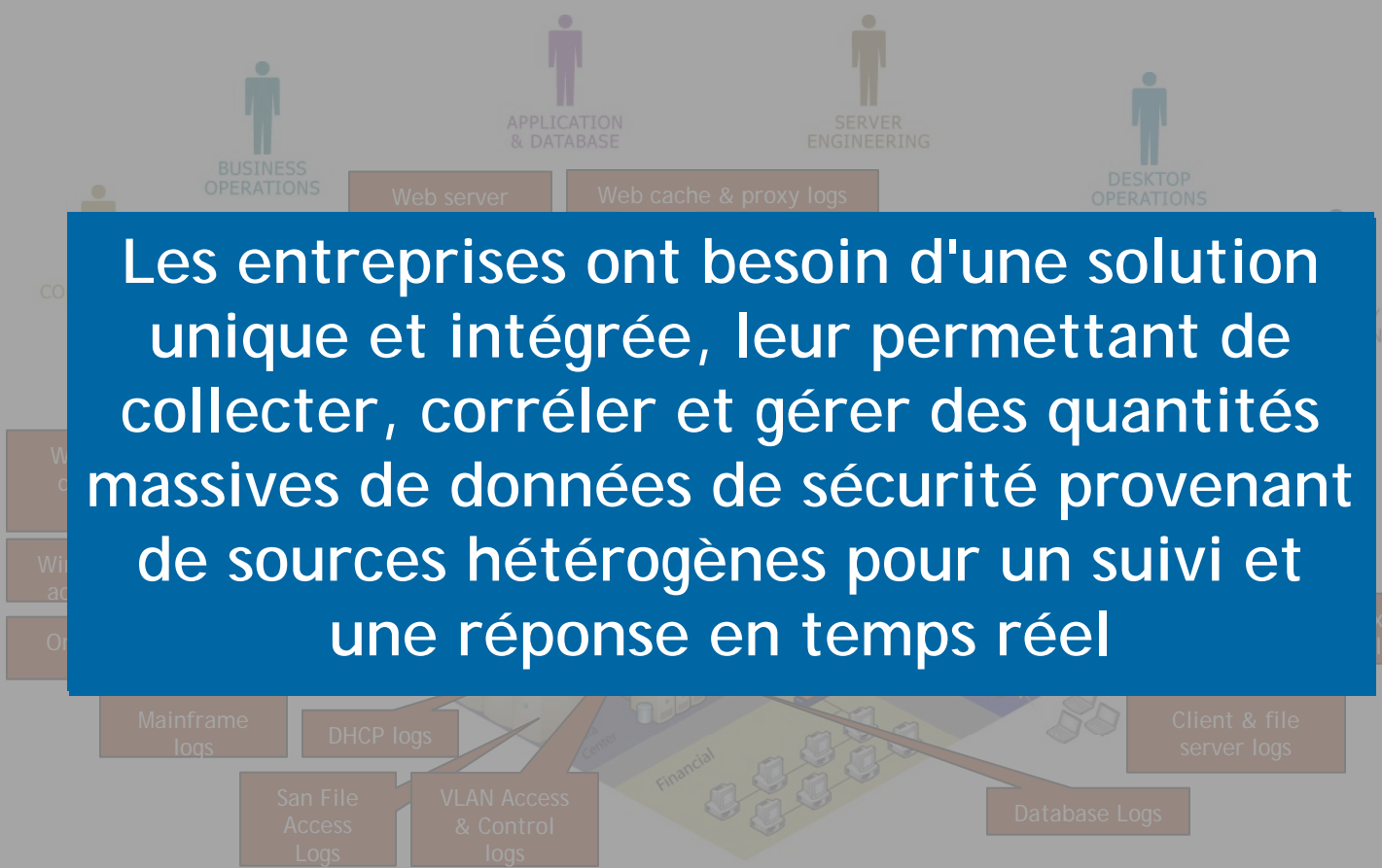
De créer un processus continue de gestion des événements

D'évaluer la capacité de la gestion de la sécurité

SIEM technology provides real-time event management and historical analysis of security data from a wide set of heterogeneous sources. This technology is used to filter incident information into data that can be acted on for the purposes of incident response and forensic analysis.

Mark Nicolette, Gartner

Les besoins



Les entreprises ont besoin d'une solution unique et intégrée, leur permettant de collecter, corrélérer et gérer des quantités massives de données de sécurité provenant de sources hétérogènes pour un suivi et une réponse en temps réel

La solution

- Il faut une solution qui s'adapte facilement à un environnement croissant et changeant;
- Un *SIEM* relie toutes les données de sécurité en un système intelligent permettant aux équipes de sécurité de gérer les exigences de conformité réglementaires, de communiquer l'état de la sécurité à un public plus large et de clarifier les menaces internes, tout en garantissant la protection du périmètre.

La solution

- 1 Journaliser tout les évènements en tout temps
- 2 Centralisation des journaux de sécurité pour l'ensemble de l'organisation de façon sécurisé
- 3 S'assurer que les données ne sont pas filtrées, éditées ou bien modifiées
- 4 S'assuré que les données sont vérifiables et authentique
- 5 Maintenir une trace auditable

Les avantages de la solution

- Collecter en continu des informations de n'importe quel type d'équipement, application, registre;
- Corréler intelligemment les informations afin d'obtenir des informations utiles dans une nuée de données;
- Contrôler la sécurité en fonction du risque organisationnel;
- Réduire fortement les délais de réponse et minimiser les dégâts;
- Stocker et extraire efficacement les informations ayant une influence sur les capacités des bases de données de l'entreprise;
- Investiguer et déterminer rapidement les causes profondes des problèmes de sécurité et des violations;
- Obtenir de manière flexible et automatique des rapports en fonction des rôles pour chaque acteur de la sécurité et de la conformité dans l'entreprise;
- Obtenir une architecture disponible et évolutive pour cette application à mission vitale;
- Gérer et personnaliser efficacement le système pour des performances élevées.

Quelques caractéristiques de la solution

Que l'entreprise dispose d'un Centre d'Opération de Sécurité 24x7 ou qu'elle désire utiliser un SIEM comme SOC virtuel automatisé, les fonctions flexibles, d'accès, d'automatisation et de personnalisation du système garantissent que l'état de sécurité est continuellement évalué et que les problèmes critiques ont l'attention méritée. Les points suivants doivent être couverts:

- Des tableaux de bord graphiques personnalisables;
- Un filtrage des événements automatisé;
- Une capacité d'effectuer la corrélation en mémoire sur des archives;
- Des graphiques d'événement dressant une image concrète et intuitive de la sécurité de l'organisation;
- Un accès simultané aux présentations en temps réel et historiques via la Console de gestion;
- Plusieurs modes de gestion des alertes (courriel, pagette, automatisation).

Architecture typique d'une solution SIEM

COMPOSÉE DE 3 COUCHES

1. Collecte de données:

- Centralisation des journaux des différentes sources d'événements;
- Collecte des journaux des différentes sources (Base de donnée, infrastructure réseau, pare-feu...)
- Normalisation des différents types de journaux (Syslog, Windows etc..);
- Chiffrement des journaux pour en assurer l'intégrité.

COLLECTE DE DONNÉES

Architecture typique d'une solution SIEM

2. Corrélation de données:

- Élimination des faux positifs par une corrélation pertinente vulnérabilité / événement;
- hiérarchisation automatique et précise basée sur criticité et gravité de l'événement et l'état de vulnérabilité;
- Règles de corrélation de base incluses et capacité de personnaliser ou de créer de nouvelles règles;
- Une corrélation en mémoire et en temps réel garantissant un traitement haute-performance;
- Des règles de corrélation indépendantes des dispositifs se fondant sur le langage de catégorisation.



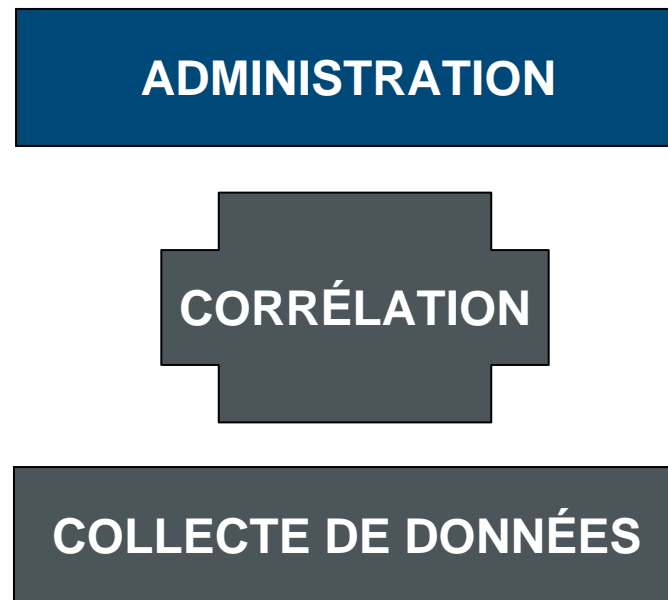
CORRÉLATION

COLLECTE DE DONNÉES

Architecture typique d'une solution SIEM

3. Administration:

- Un accès simultané aux présentations en temps réel et historiques via la Console ou un accès sécurisé, à n'importe quel moment, n'importe où via le Web;
- Des tableaux de bord graphiques personnalisables qui offrent une présentation par activité, zone géographique et rôle technique;
- Des graphiques d'événement dressent une image concrète et intuitive de la sécurité de l'organisation;
- La programmation et la distribution automatisées de rapports;
- Gestion granulaire des utilisateurs pour assurer une gestion des droits d'accès précise.



Les bénéfices d'un SIEM

- La mise en place d'un SIEM permet aux organisations:
 - d'obtenir une vue sur l'ensemble l'état de leur infrastructure en temps réel;
 - réduire le temps de réaction en cas d'incident;
 - de rencontrer un très grand nombre d'obligations légales et contractuelles;
 - de pouvoir soutenir de manière non équivoque les processus d'enquêtes sur les cyber incidents;
 - de diminuer les risques liés au réseau et aux technologies de l'information.

Les bénéfices d'un SIEM

La mise en place d'un SIEM permet aux organisations:

1

D'obtenir une vue sur l'ensemble de l'état de leur infrastructure en temps réel

2

Réduire le temps de réaction en cas d'incident

3

De rencontrer un très grand nombre d'obligations légales et contractuelles

4

De pouvoir soutenir de manière non équivoque les processus d'enquêtes sur les cyber incidents

5

De diminuer les risques liés aux réseaux et aux technologies de l'information

Merci

André Beaudoin
andre.beaudoin@bell.ca