



WebSphere



Maitrise du Risque et Lutte contre la Fraude : les nouveaux défis

*Christophe Herman,
Solutions Métier - Software Group IBM*

1^{er} et 2 octobre 2007



Maitrise du Risque et Lutte contre la Fraude : les nouveaux défis

- Agenda :
 - Le contexte
 - La solution EAS – GNR
 - La solution Consul Insight



Le risque, une notion toute relative mais cruciale pour les organisations ...



- Probabilité que survienne un évènement néfaste pour une organisation
- Les types de risques et leur impacts potentiel varient suivant les organisations



Informatique, Conformité et Lutte contre la Fraude au cœur des préoccupations des Directions « Maîtrise des Risques »

Table 2. Percentage of responses among operational risk managers to the query, "Please rank the top five operational risks in terms of their impact on the organization." (Source: OpRisk & Compliance Magazine, 1 April 2006)

	2005	2006
<i>Risk Category</i>	<i>Total</i>	<i>Total</i>
IT systems failure / inadequate MIS	60.7%	60.8%
Transaction processing failures	-	48.6%
Regulatory / compliance	61.3%	44.6%
External fraud	38.7%	44.6%
Internal fraud	25.6%	43.2%
Customer relationship risk	37.5%	31.1%
Legal liability	16.1%	28.4%
Business continuity / terrorism	46.4%	28.4%
Lack of internal transparency on op risk information	17.3%	25.7%
Financial accounting / reporting	19.6%	25.7%
Anti-money laundering	38.1%	24.3%
Key person retention	20.2%	21.6%
Inadequate financial controls	23.8%	21.6%
Political / country risk	4.8%	6.8%
Loss / damage to physical assets	6.0%	14.9%
Inability to attract high-quality staff	16.1%	18.9%
Taxation	2.4%	4.1%

Problématiques fortes
quel que soit
le Secteur d'activités

Problématiques fortes
en particulier pour
le Secteur Public



La maîtrise du risque : exemple du Secteur Public



La Fraude dans le Secteur Public : quelques chiffres ...



- **La contrefaçon**
 - 300 M€ saisis par les Douanes (2005)



- **La fraude à l'identité**
 - 600 000 cartes d'identité disparues en 2006



- **La fraude sociale (fraudes et abus)**
 - 2 Milliards €, voire plus !

- **La fraude fiscale**
 - 45 Milliards € (*)



(*) Estimation du Syndicat national Unifié des Impôts)

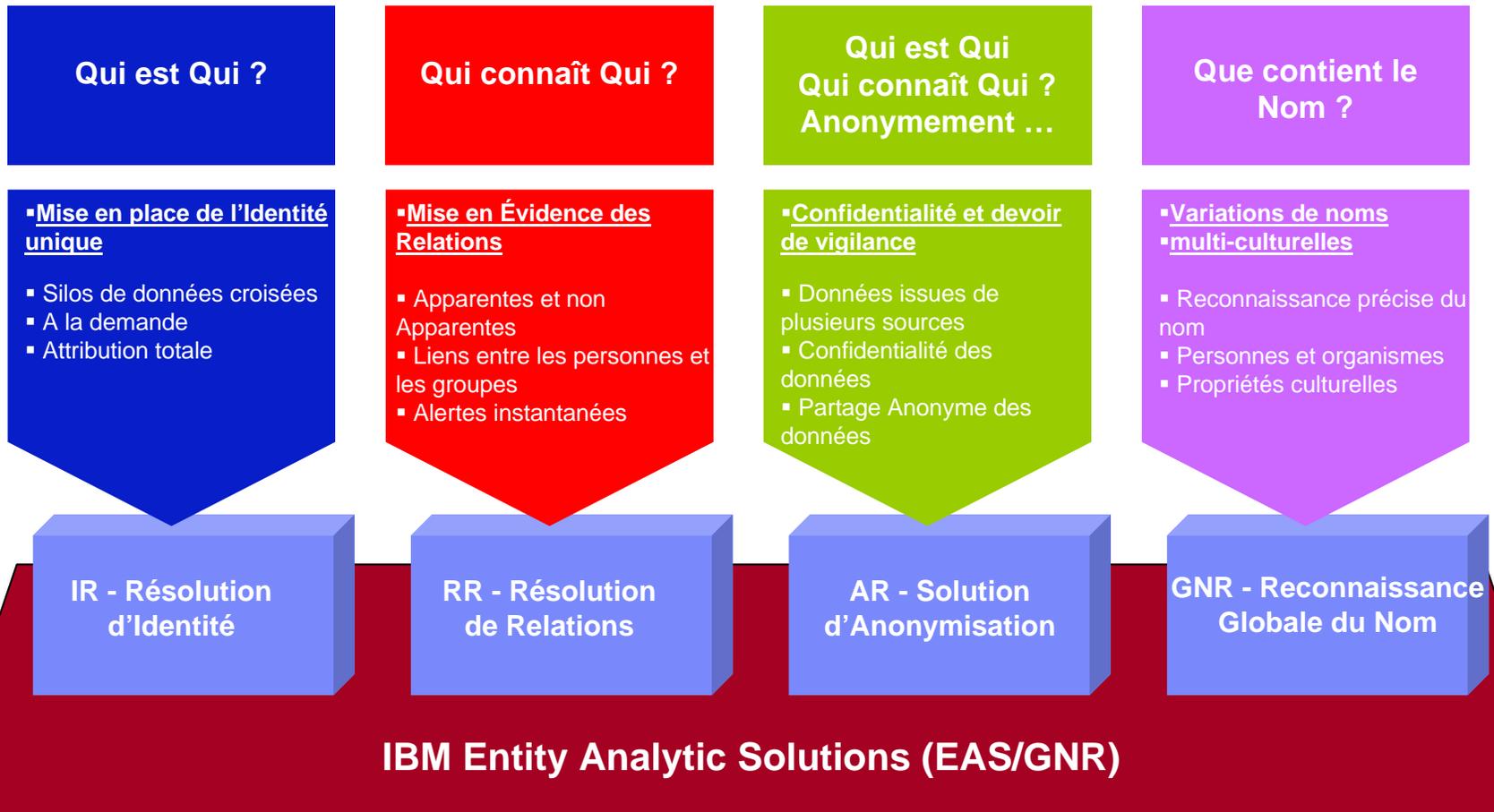


Intensification de la fraude : un contexte global

- La résolution des identités : un fondement de l'analyse de la fraude / criminalité
- L'identification de relations non évidentes entre personnes / entités (sociétés, groupes) est une exigence pour lutter contre la fraude / criminalité
- Il est nécessaire d'anticiper / de travailler de plus en plus en temps réel
- Les organismes publics / privés sont amenés à collaborer étroitement



La solution IBM anti-fraude EAS/GNR



1er Module : “R.I. Résolution d’Identité” – Aide à répondre à la question « Qui est qui ? »

Ce module permet de reconnaître une personne physique ou morale utilisant de multiples identités



Dr Katrin Dupont
1 Ave Dumesnil
78230 Saint-Cloud
Tel :01 49 05 50 84
Id : 2640809737615
DDN :07/08/64
GSM : 068588345



Dr Cathy Dupond
10 rue Saint-Martin
Chatillon 51700
Tel : 03 49 05 50 84
GSM : 068588345



Mme Catherine Dupond
1 rue de Bourgogne
Châtillon 51700
Tel :03 49 05 60 55
DDN : 07/09/66
Id : 2660973761563



Mme Katrin Dubois
Tour Europa Appt B24
La Défense, 92066
Tel : 01 45 65 45 40
DDN : 07/08/64
Id : 2640809737615

2ème module “R.R. Relationship Resolution”

Aide à répondre à la question : “Qui connaît qui” ?

(Règle associative: si $A \Leftrightarrow B \Leftrightarrow C$, alors $A \Leftrightarrow C$)



A: Mark Smith

Phone: (713) 730 5769



B: Kate Green

Phone: (713) 730 5769

Addr: 123 Main St



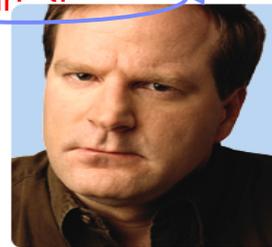
C: Tom Sinclair

Addr: 123 Main St



A: Mark Smith

Phone: (713) 730 5769



C: Tom Sinclair

Addr: 123 Main St



Mark est en relation avec Tom avec 2 degrés de séparation.

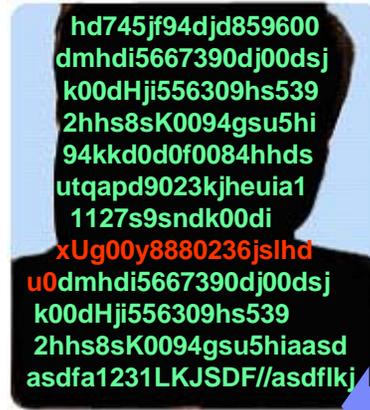
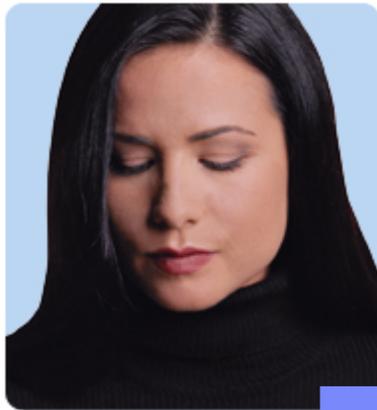
EAS gère jusqu'à 30 degrés de séparation!



3ème Module « A.R. - Solution d'Anonymisation »

Détermine "Qui est qui et qui connaît qui... en respectant l'anonymat"

Permet à plusieurs intervenants de partager et de comparer des informations rendues anonymes, issues de plusieurs sources



Catherine Dupond
 1 rue de Bourgogne
 Chatillez 51700
 VIN# 585789543
Frequence Plus: 5678965
 Tel: 03 49 05 60 55
 Passeport : 995027890

tr5y9hU000kdG563ks
 Hjd55603jd98hj4jklf9jt
 0089gehyud98kkdh00
 Hydk8880h332jd78001
xug00y8880236jslhdu0
 0012g6743kd85hf06h7
 x084hdf75jc4539fhd89

hd745jf94djd859600dm
 hdi5667390dj00dsjk00d
 Hji556309hs5392hhs8s
 K0094gsu5hi94kkd0d0f
 0084hhdsutqapd9023kj
 heuia11127s9sndk00di
xug00y8880236jslhdu0

Thomas Saint-Clair
 49 Rue Basse
 Louveciennes 78120
 Compte n° : 97836553122
 Compte n° : 00303450009
 Tel : 01 50 16 03 82
Frequence Plus: 5678965

4ème module Global Name Recognition:

Exemple, le même nom en Asie du Sud-Est



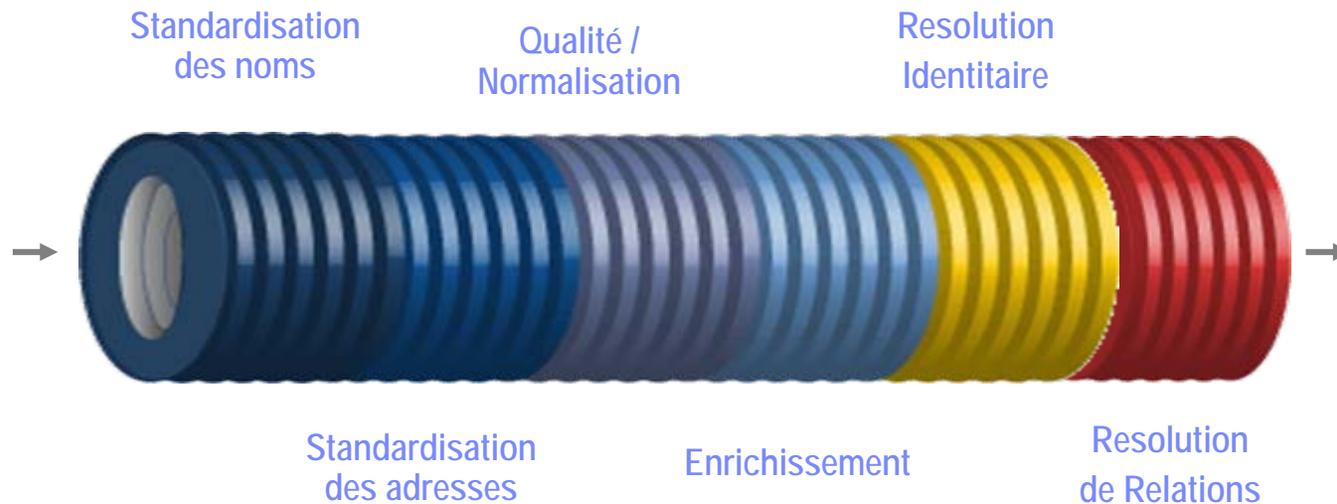
張
丘
蘇

China ★ Passport	Zhang Qiusu
Taiwan T ★ Passport	Chang Ch'iu-Su
Thailand T ★ Passport	Chiusu Sae
Singapore Sin ★ Passport	Chang Cheung Yau So
Malaysia M ★ Passport	Cheung Yau So

- Un attribut unique pour le nom et les prénoms au lieu de plusieurs
- Base de connaissance de près d'1 milliards de noms
 - Grâce à 20 années de recherche linguistique informatique
- Règles basées sur la culture spécifique de chaque nom pour obtenir de meilleurs rapprochements, recherches, analyses grammaticales et de scores



De plus, EAS émet des alertes en temps réel, ce qui permet de mettre en oeuvre une gestion préventive de la fraude



- 5,000 sources de données +
- 500 millions + d'entités résolues
- 3 milliards + de lignes de B.D.
- Débit (fil de l'eau) jusqu'à 2200 ERPS
(Entités Résolues par seconde)



Consul Insight, une solution unique pour la gestion du risque de non conformité face aux exigences de sécurité informatique

- Consul InSight collecte, consolide, effectue des corrélations automatiques entre l'ensemble des accès au S.I. et remonte les alertes pertinentes relatives à aux anomalies concernant la sécurité interne
- Consul Insight favorise la prise en compte des procédures qui peuvent être facilement paramétrées, la production de tableaux de bord et d'états plus détaillés
- Consul Insight facilite les investigations nécessaires en matière de sécurité ainsi que leur remédiation, offre des fonctionnalités uniques en terme d'auditabilité des accès au S.I. afin de réduire drastiquement les risques de fraude interne

- **Renforcer la sécurité du S.I. de bout en bout**
- **Réduire les risques relatifs à la fraude interne**



A propos de Consul...

Experts dans l'audit de sécurité et la compliance depuis 1986

- Créée en 1986
- Siège mondial à Herndon (Virginia), siège Europe aux Pays Bas
- Acquisée par IBM en 2007

Choisie par plus de 350 clients dans le monde



Reconnu par la presse et les analystes



Il faut monitorer les accès anormaux au S.I. (B.D., Réseau, ...) selon des seuils acceptables pour les différents utilisateurs



Massive Insider Breach At DuPont

A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706

The Delaware U.S. attorney on Thursday revealed a massive insider data breach at chemicals company DuPont where a former scientist late last year pleaded guilty to trying to steal \$400 million worth of company trade secrets. He now faces up to a decade in prison, a fine of \$250,000, and restitution when sentenced in March.

Commentaires de la CIA:

"...les concepteurs et les scientifiques tendent à regarder la propriété intellectuelle de leur compagnie comme leur propre... et quelque chose qu'ils veulent prendre avec eux "

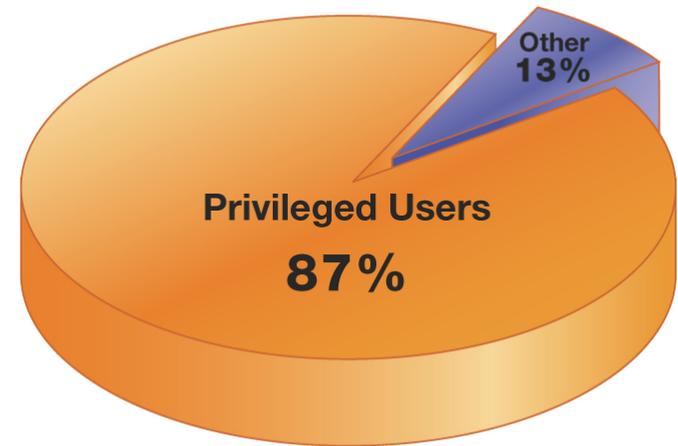
Source: InformationWeek, Feb. 15, 2007



La surveillance des utilisateurs privilégiés (PUMA) n'est plus facultative !

- 87% des délits d'initiés sont causés par des utilisateurs privilégiés et techniques
- Cela coûte trop cher d'ignorer que:
 - Les attaques internes ont coûté 6% du revenu annuel brut
 - Soit \$400 milliards uniquement pour les USA

Who Causes Internal Incidents?

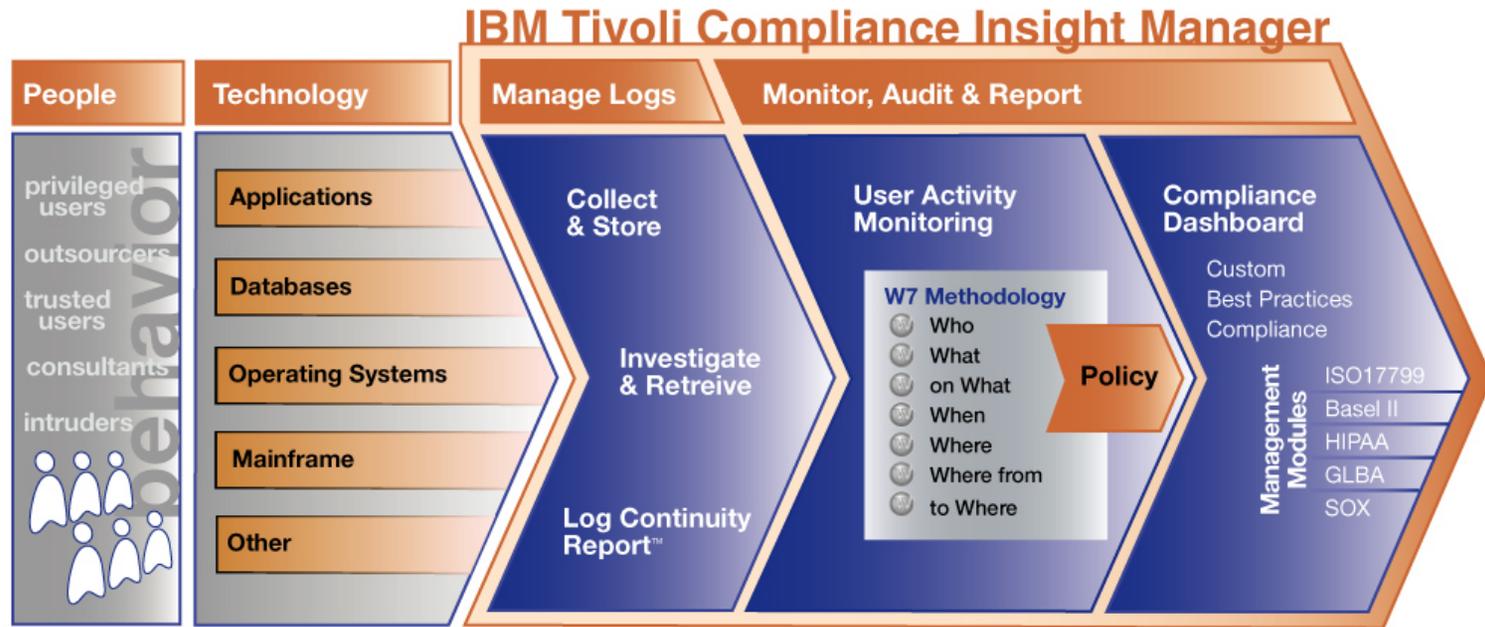


Source: USSS/CERT Insider Threat Survey 2005

Les experts, analystes, auditeurs, et organismes de régulation demandent aux entreprises de se prémunir activement face à ce type de risque



Reporting complet d'audit et de conformité



Possibilités:

- Centaines de rapports
- Modules de conformité
- Alertes d'attention spéciale
- Rapports douaniers

Bénéfices:

- Réduction du temps et de l'effort nécessaire lors d'audit
- Réduction du risque d'une menace interne:
 - Protection de l'information
 - Contrôle du changement
 - Gestion de l'utilisateur

Tableau de Bord "Compliance"

[Dashboard](#)
[Trends](#)
[Reports](#)
[Regulations](#)
[Policy](#)
[Groups](#)
[Distribution](#)
[Settings](#)

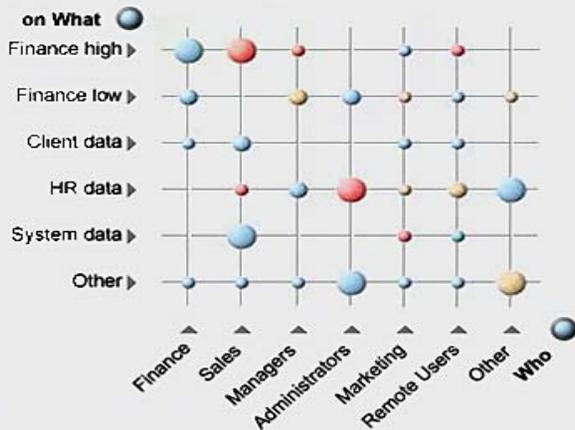
EPRORADB Portal

Compliance Dashboard Database AGGRDB on Server EPRORADB

Enterprise Overview

Settings

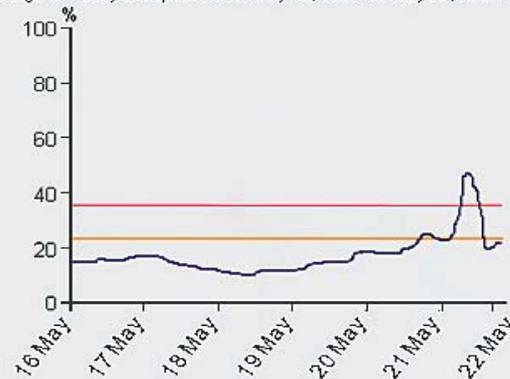
Events by top event count by "Who" and "on What" from May 16, 2007 till May 22, 2007.



Trend graphic

Settings

Percentage of Policy Exceptions from May 16, 2007 till May 22, 2007.



Database Overview



AggrDb



SelfAudit

Name: SelfAudit
Status: Database loaded successfully
Loading date: Sun May 13 2007 20:00:53 GMT+02:00
Content: 192.168.88.133 (InSightPortal), INSIGHTTEST (InSight, Unavailable, iView), INSIGHTTEST\INSIGHTTEST (Windows)
Automatic policy: Sun May 13 2007 19:58:27 GMT+02:00
User policy: Sat Jan 01 2000 01:00:00 GMT+01:00



Compliance Modules

Basel II

Introduction | Classification Template | Policy Template | Reports | Documentation

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

ISO 17799

Introduction | Classification Template | Policy Template | Reports | Documentation

Sarbanes Oxley (SOX)

Introduction | Classification Template | Policy Template | Reports | Documentation

Classification Template

Download the template to use in the management Console.

Who: [dropdown]
What: [dropdown]

Group Name	Description
Alerts	Alerts generated by system devices resources
Alerts - High	Alerts generated by system devices resources - High
Alerts - Low	Alerts generated by system devices resources - Low
Alerts - Medium	Alerts generated by system devices resources - Medium
Exposure - High	Description of Exposure - High
Exposure - Low	Description of Exposure - Low
Exposure - Medium	Description of Exposure - Medium
Intrusion - High	Description of Intrusion - High
Intrusion - Low	Description of Intrusion - Low
Intrusion - Medium	Description of Intrusion - Medium
Intrusions	Intrusions reported by IDS devices

Who: [dropdown]
Where: [dropdown]

Group Name	Description
Office Hours	Normal working hours for staff
Out of Office Hours	Out of normal working hours
Weekend	Non-working days

Extra Information

Help

In the US:
contact@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077

EMA and Asia Pac:
contact@consul.com
Direct Line: +31 16 261 3333

@consul.com
1 703 675 2022

Policy Template

Download the template to use in the management Console.

Policy Rules

Attention Rules

Who group	What group	Where group	Where group	What group	Where's Group ID	Severity	Description
HR Management	Intrusion - Medium			Remote Intrusion		30	Review attention
Administrators	Customer Information Systems	HR - Medium				40	Review attention
Administrators	Financial	Medium				50	Review attention
Administrators	Customer Data	High				50	Review attention
Administrators	Financial	Low				70	Requires immediate attention
IT	Sensitive					20	Review
Database	Customer					25	Review

Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFEC 1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFEC 1.2.1.1) Classification report	No description supplied
Sarbanes Oxley (8.2.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.
Sarbanes Oxley (8.1.2) Operational change control	Changes to the operating environment such as system updates, DSA activity etc.
Sarbanes Oxley (8.1.6) External contractors	Exceptions and failures caused by External Contractors
Sarbanes Oxley (8.2) Database activities	Exceptions and failures due to Database activities
Sarbanes Oxley (8.4.2) Operable log	Actions performed by the IT Admin staff
Sarbanes Oxley (8.5) Network management	Actions and failures caused by users on Network Services
Sarbanes Oxley (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets
Sarbanes Oxley (8.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data
Sarbanes Oxley (8.2.4.8.2) Review of user access rights	Actions performed by administrators on users
Sarbanes Oxley (8.2.4.6.3.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (8.2) User responsibilities and password use	Login failures and successes either locally or remotely.
Sarbanes Oxley (8.4) Network access control	Actions performed on and events and exceptions generated by Network or Router
Sarbanes Oxley (8.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (8.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers
Sarbanes Oxley (8.5.2) User identification and authentication	Login/Logout successes and failures
Sarbanes Oxley (8.5.5) System utilities	Usage of system utilities
Sarbanes Oxley (8.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data
Sarbanes Oxley (8.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully
Sarbanes Oxley (8.6.2) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data
Sarbanes Oxley (8.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the iRights system
Sarbanes Oxley (8.8.1) Update control	Exceptions and failures for update control

TEC - Technical Exploration Center - @ Paris

Accélérer le cycle de découverte des logiciels IBM

Les ressources hardware et software du TEC à Noisy-Le Grand / Marne La Vallée sont disponibles **gratuitement** :

« Les équipes Sales et TechSales de IBM Software, sont à votre disposition pour réserver des machines et des ateliers »

– EOTs - Exploration of Technology

- Découvrir la valeur des logiciels IBM: Présentations, vidéos, démonstrations

– POTs – Proof of Technology, Ateliers/Workshops,

- Démontrer les capacités des logiciels IBM
 - Présentations
 - Labs et hands-on ...

une adresse E-mail à retenir:
TecParis@fr.ibm.com

NEW

You're invited

Discovering the value of IBM Tivoli Compliance Solutions

AN IBM PROOF OF TECHNOLOGY

