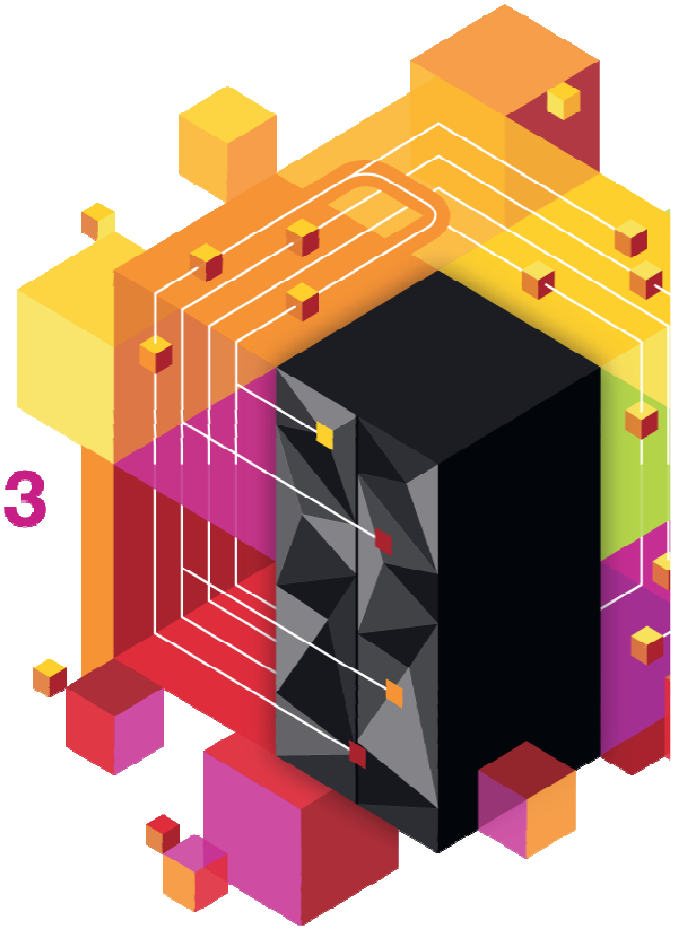
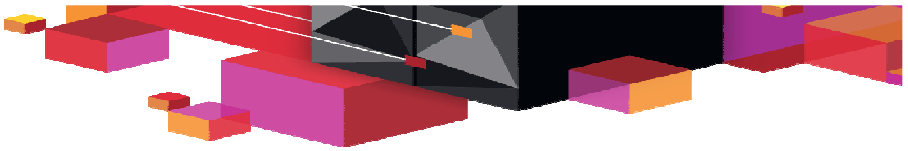
Université du Mainframe 2013

4-5 avril





Sécurisation des données métiers

Serge Richard – CISSP®
Architecte Solutions de Sécurité
serge.richard@fr.ibm.com

Stéphane LY
Consultant de Sécurité Mainframe
Stephane_ly@fr.ibm.com

Université du Mainframe 2013

4-5 avril

Agenda

- Défi et enjeux de la sécurisation des données métiers
- Stratégie client et Offres IBM
  - Pourquoi la sécurité sur Mainframe ?
  - Protection des données sur la plateforme z
- Démonstrations
  - Qradar, zSecure et Guardium
- Questions / réponses

Défi et enjeux de la sécurisation des données métiers

Problématiques

Prévenir des fuites de données

- Atténuer les menaces internes ou externes sur l'ensemble des environnements (prod, pre-prod, recette, dev).
- Empêcher la divulgation ou la perte de données sensibles

Maintenir l'intégrité des données

- Prévenir des tentatives de modifications non autorisées sur les données ou les structures

Réduire les coûts liés à la conformité

- Automatiser et centraliser les contrôles

Exemples de cas clients

Exemples d'attaques

Heartland Payment Systems — The Highest Standards | The Most Trusted Transactions
100M credit cards stolen

citi
200K+ account records stolen

92% des cas de compromission reposent sur les bases de données

epsilon
Customer data of 2.5K brands lost

SK telecom
35M on-line accounts stolen

Exemple de projets

Administration fiscale	Prévenir des fuites d'informations	Détection des activité inappropriées par les utilisateurs à fort privilèges. De meilleurs contrôles permettent de prévenir la fuite de données
Compagnie d'assurance	Maintenir l'intégrité des données sensibles	Mise en place d'utilisateurs à accès privilégiés Suivi et la réconciliation des activités DBA
Entreprise financière	Réduire le coût de la conformité	Réduction des coûts opérationnels pour répondre au besoin de conformité
	Gérer la conformité	Mise en place d'un chiffrement automatique des données pour assurer la protection des données et cela dans le respect des coûts

Approche holistique pour une solution sur la sécurité des données

Comprendre et définir les données sensibles
Comprendre où elles résident, comment elle sont liées et comment définir les politiques et métriques pour protéger celles-ci

Surveiller et auditer
Surveiller les processus et transactions, renforcer les politiques et mettre en place des audits détaillés

Gérer les accès
Gérer les priviléges et authentifier les utilisateurs pour limiter l'accès aux données

Evaluer les vulnérabilités
Détecter les vulnérabilités pour protéger les environnements contenant les données sensibles

Prévenir des activités non autorisées
Bloquer les transactions qui ne respectent pas les politiques de sécurité

Chiffrer les données
Chiffrer les données sensibles, structurées ou non structurées, pour les protéger contre des lectures non autorisées

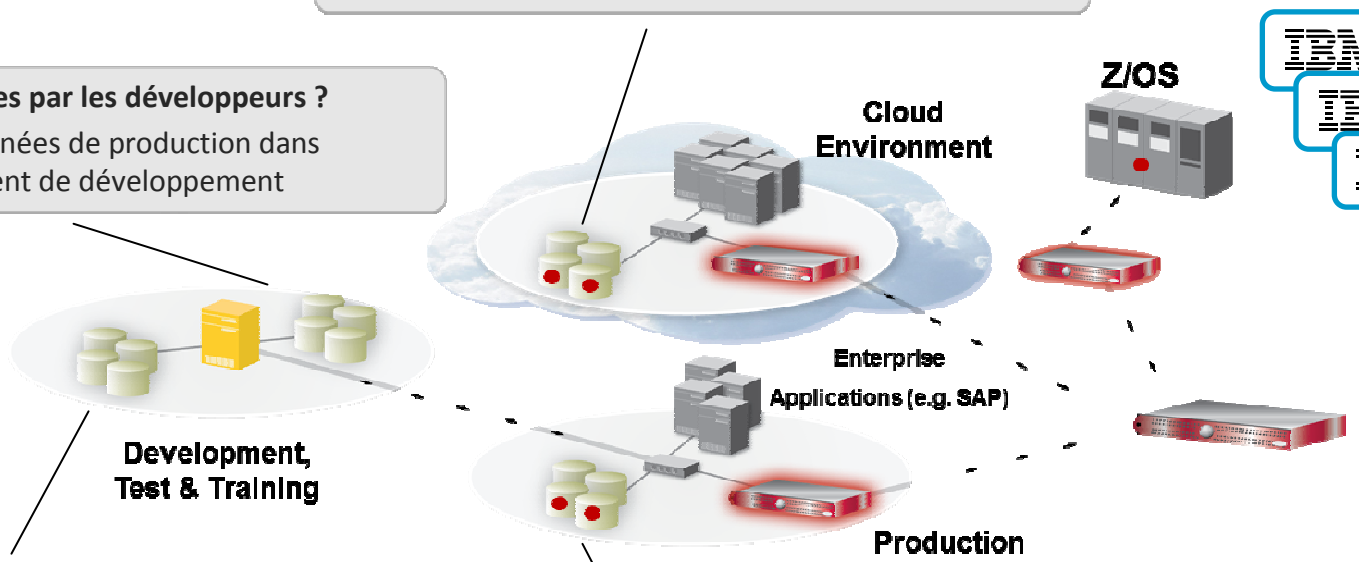
Protéger les données sensibles dans les environnements de non production
Masquer la donnée par des techniques d'anonymisation

Protéger les données non structurées
Expurger les données sensibles des fichiers

Challenge 1: Protéger les données

Accès des utilisateurs à privilèges ?
Ils peuvent facilement contourner les protections

Vol de données par les développeurs ?
Copie des données de production dans l'environnement de développement



Mauvaises configurations ?
Facilite les accès aux pirates

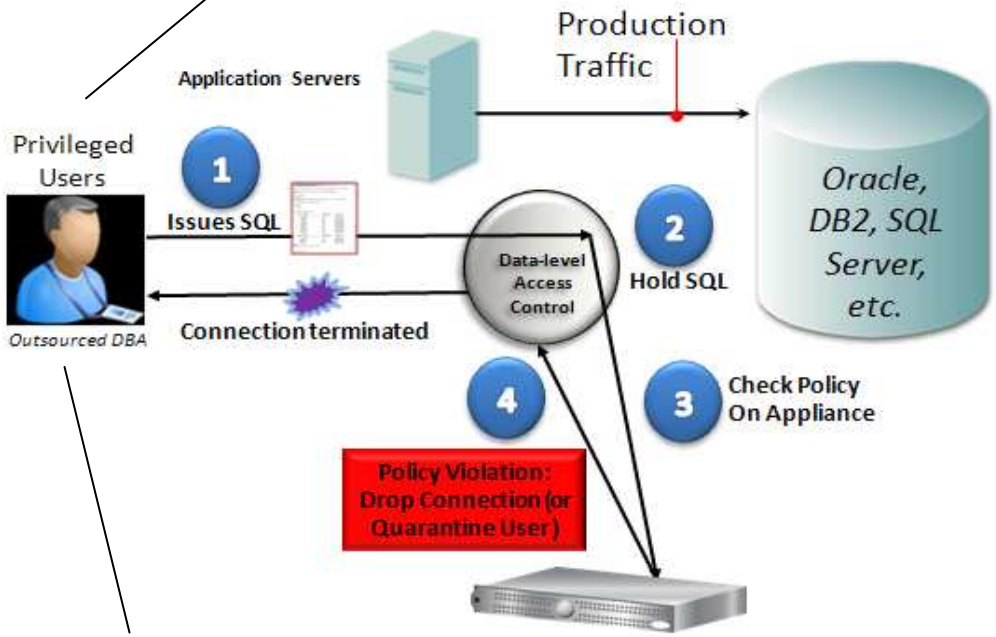
Fraude commise par un utilisateur ?
Manque d'information sur l'activité utilisateur (signaux faibles)

- Surveiller les transactions sans avoir à modifier les bases de données ou les applications
- Anonymiser les jeux de test
- Chiffrer les données pour prévenir du vol (archive, backup,…)
- Expurger les informations sensibles des données non structurées

Challenge 2: Maintenir de l'intégrité des données sensibles

Les utilisateurs privilégiés ou le personnel en sous-traitance peuvent effectuer des modifications non autorisées ?

La plupart des organisations n'ont aucun contrôle sur les actions des DBA, et aucun moyen de les contrôler efficacement



Les utilisateurs contournent les protections des applications ?

Les mécanismes d'identification et d'authentification aux applications sont connus des utilisateurs, les entreprises n'ont pas les moyens de contrôler les actions de contournement de ces protections

Contrôler les transactions par rapport aux politiques et bloquer les violations en temps réel

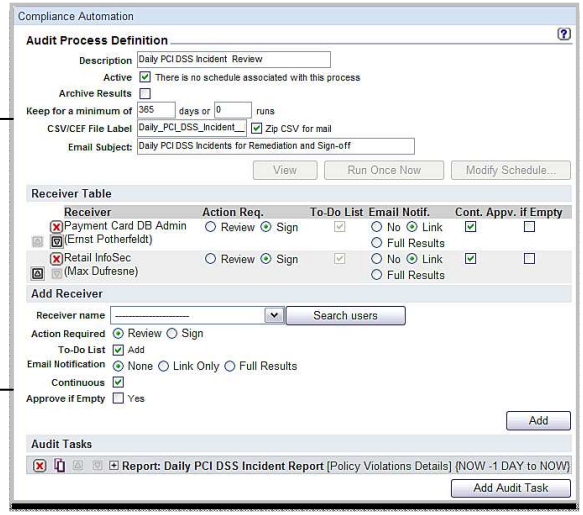
```
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel

SQL>
```

Session Terminated

Challenge 3: Réduire les coûts liés à la conformité

Est il nécessaire de fournir des données associées à une preuve de conformité ?

Permettre une agrégation des différents éléments en un point centralisé. Permettre la rédaction de rapport spécifique à chaque besoin de conformité et cela dans le but de simplifier les audits

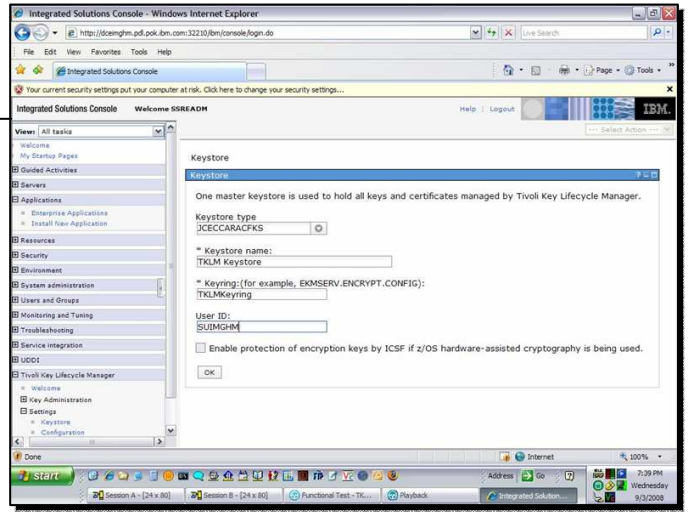


Est ce que les violations des politiques sont détectées ?

Montrer que ces violations peuvent être détectées et traitées. Et cela au travers de processus automatisés par des outils de surveillance (SIEM)

Est ce que le chiffrement est demandé pour la conformité ?

Automatiser et centraliser la gestion des clés et simplifier l'implémentation du chiffrement



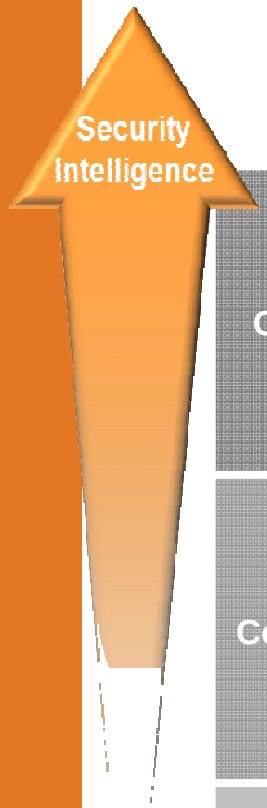
Automatiser et centraliser les processus liés à la conformité

Les organisations ont besoin d'une approche de la sécurité des données et de la conformité à l'échelle de l'entreprise

Comprendre et définir les données sensibles	Evaluer les vulnérabilités	Surveiller l'activité sur les bases de données	Protéger les données sensibles	Gérer les accès
Automatiser la détection des données sensibles et le schéma de relation entre les données	***Automatiser la détection des vulnérabilités et des changements de configuration sur des bases de données***	***Fournir des garanties pour protéger les bases de données de grande valeur dans des environnements hétérogènes***	***Protéger les données dans les environnements de production et de non-production***	***Gérer et appliquer les politiques sur l'ensemble de l'entreprise***
Capacités : ✓Découverte des instances des bases de données ✓Découverte des données sensibles ✓Automatiser les actions sensibles	**Capacités** : ✓Automatiser la recherche de vulnérabilités ✓Auditer les changements	**Capacités** : ✓Contrôle des activités sur les bases de données en temps réel ✓Audits ✓ Politiques permettant de surveiller les accès et les actions non autorisées	**Capacités** : ✓Anonymiser les données ✓Automatiser le processus de gestion de clefs ✓ Chiffrement ✓ Expurger les donnés sensibles des documents	**Capacités** : ✓Centraliser et automatiser la collecte des informations ✓Evaluer les accès à risque
			IBM Key Lifecycle Manager	
			Infosphere Guardium Data Encryption	
Infosphere Guardium Data Finder		**Security Qradar SIEM**	**Infosphere Optim Data Masking**	**Security Qradar SIEM**
Infosphere Data Discovery	**Infosphere Guardium Vulnerability Assessment**	**Infosphere Guardium Data Activity Monitoring**	**Infosphere Guardium Data Redaction**	**Infosphere Guardium Entitlement Reports**

Addresser les besoins liés à la conformité

Aider les entreprises a évoluer dans leur maturité



	Individus	Données	Applications	Infrastructures	Security Intelligence
Optimisé	Role based analytics Identity governance Privileged user controls	Analyse flux de données Gouvernance des données	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Securing systems	Advanced threat detection Network anomaly detection Predictive risk management
Compétent	User provisioning Access mgmt Strong authentication	Gestion des accès Prévention perte des données	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management	Real-time event correlation Network forensics
Basic	Centralized directory	Chiffrement Contrôle d'accès	Application scanning	Perimeter security Anti-virus	Log management Compliance reporting

Stratégie de sécurité sur Mainframe

- Le Mainframe est la plateforme la plus sûre au monde
  - La sécurité est une caractéristique de base du System z
  - Il y a un ensemble des fonctions de sécurité intégrées (z/OS et RACF)

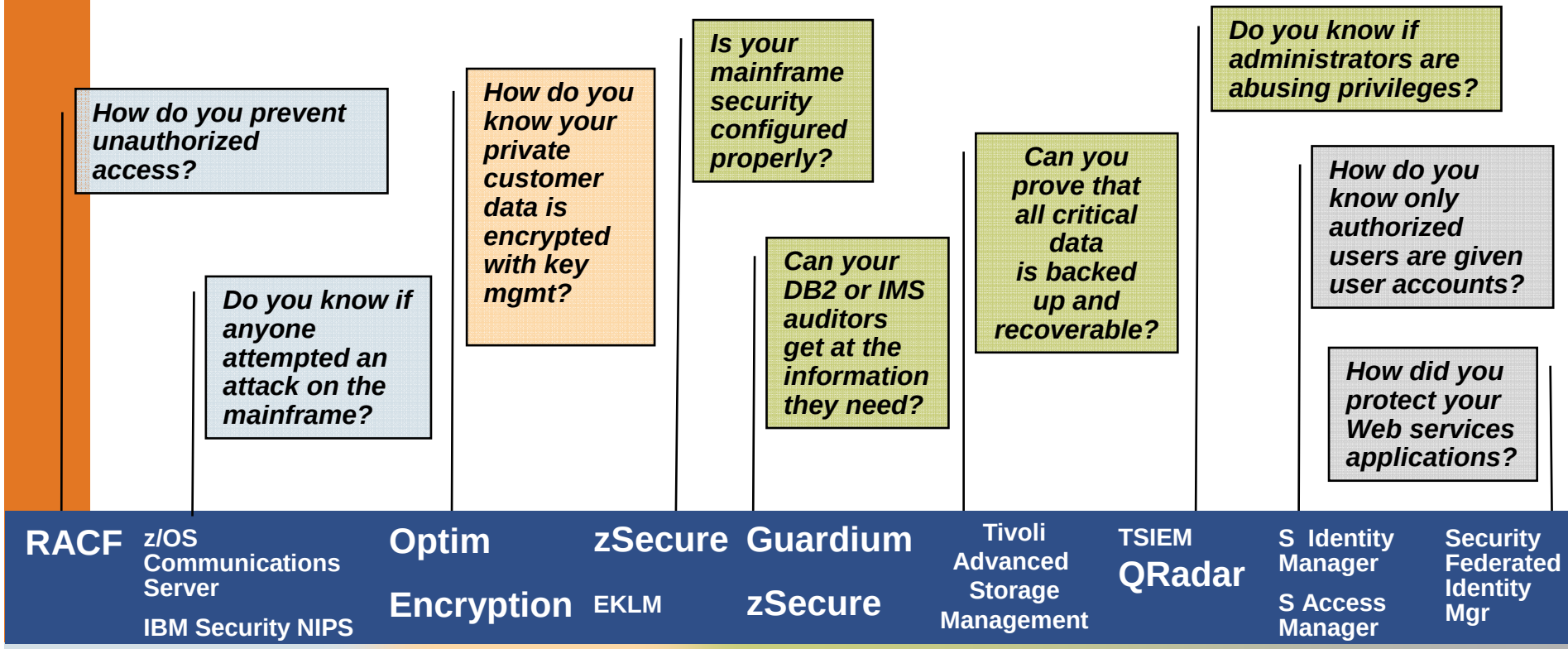
- Cela ne dispense pas de définir une stratégie globale et cohérente
  - qui vise à avoir le plus haut niveau de sécurité avec des contrôles permanents,
  - une visibilité globale de sécurité «de bout en bout»,
  - tout en simplifiant la gestion

- Cette stratégie doit s'appuyer sur des **outils** qui permettent :
  - Une **politique renforcée face à la montée des menaces, et simple** à mettre en œuvre (sur les volets administration, audit, monitoring, alertes, prévention et sur toute la chaîne de sécurité : gestion des accès, audit en amont, mesures en aval…)
  - Une politique qui protège tout particulièrement les **données critiques** (chiffrement à grande vitesse, gestion centralisée des clés de chiffrement…)

La sécurité : ADN du System z

- «Sécurité» est incorporée de la conception à la construction du System z
  - Hardware
    - Etanchéité absolue de plusieurs partitions ou machines virtuelles (certifié EAL 5)
  - Firmware
    - Protection de mémoires réelles ou de mémoires virtuelles par clé
  - Hypervisors
    - PR/SM (certifié EAL5)
  - System z Operating Systems
    - z/OS, z/VM & Linux avec RACF (certifié EAL5)
  - Middleware et applications
    - CICS, IMS, WebSphere et DB2 intégrés avec RACF
  - Réseaux
    - HiperSockets : communications entre plusieurs partitions ou machines virtuelles
- Le System z est au cœur des offre stratégiques de IBM :
  - Smarter City, Smart Cloud Entreprise, BigData, Business Analytics …

Panorama des solutions IBM en matière de sécurité

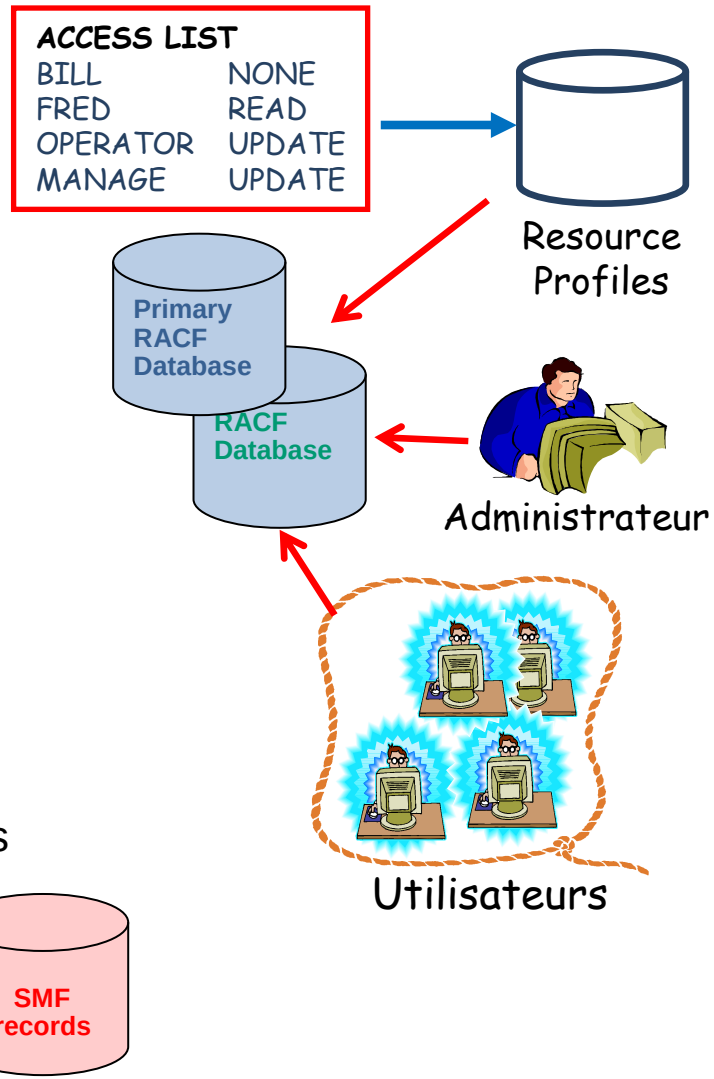


*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

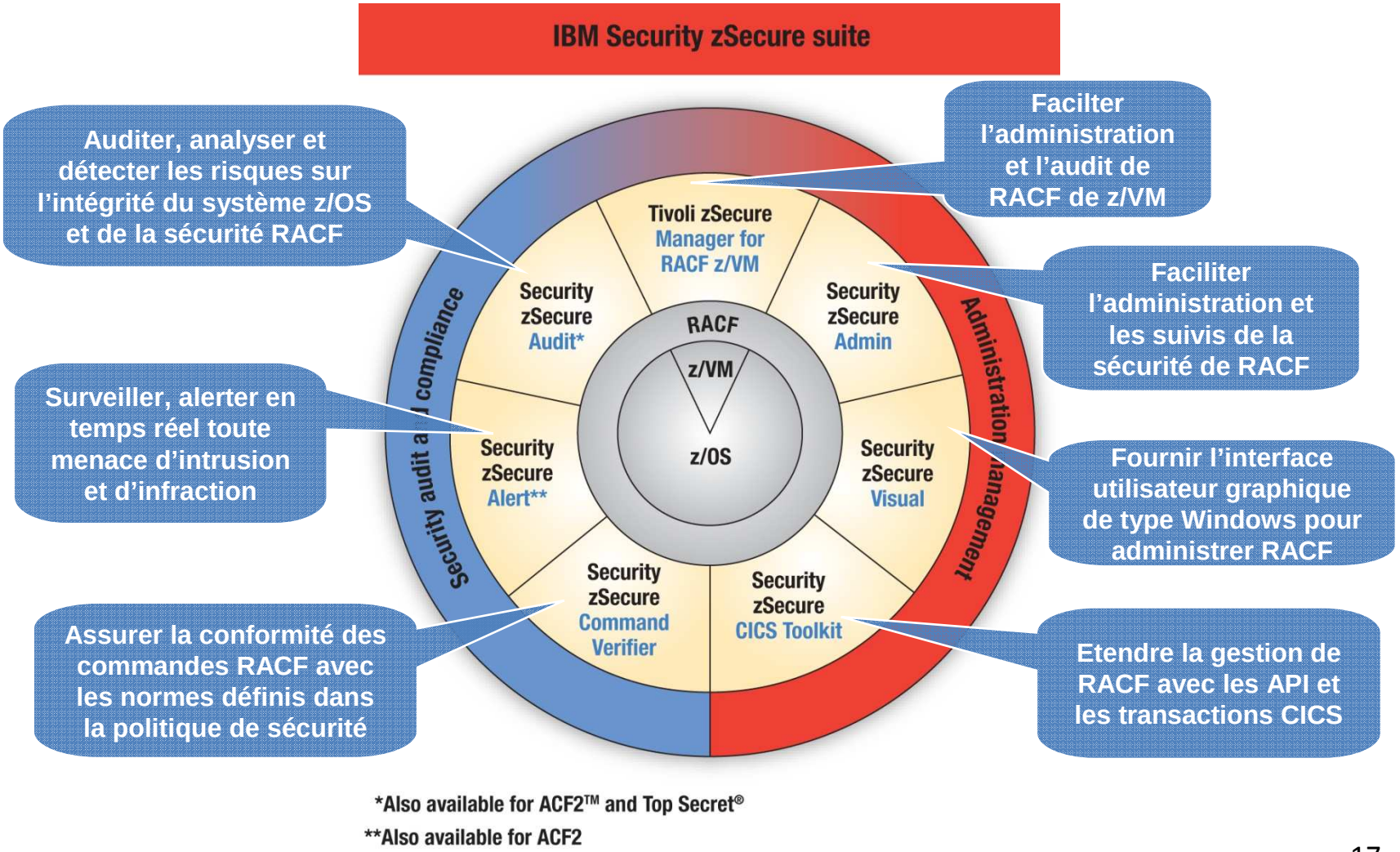
RACF (Resource Access Control Facility)

- Epine dorsale de la sécurité z/OS
- Gestion et administration de la politique de sécurité
- Identification et authentification des utilisateurs
- Contrôle des accès aux ressources
  - Composants systèmes
  - Sous-systèmes
  - Applications
  - Données

  zOS, TSO, CICS, WAS, IMS, DB2, TCP/IP
- Journalisation des actes d'administration, activités des utilisateurs, accès aux ressources, ou toutes déviations à la politique de sécurité d'entreprise.

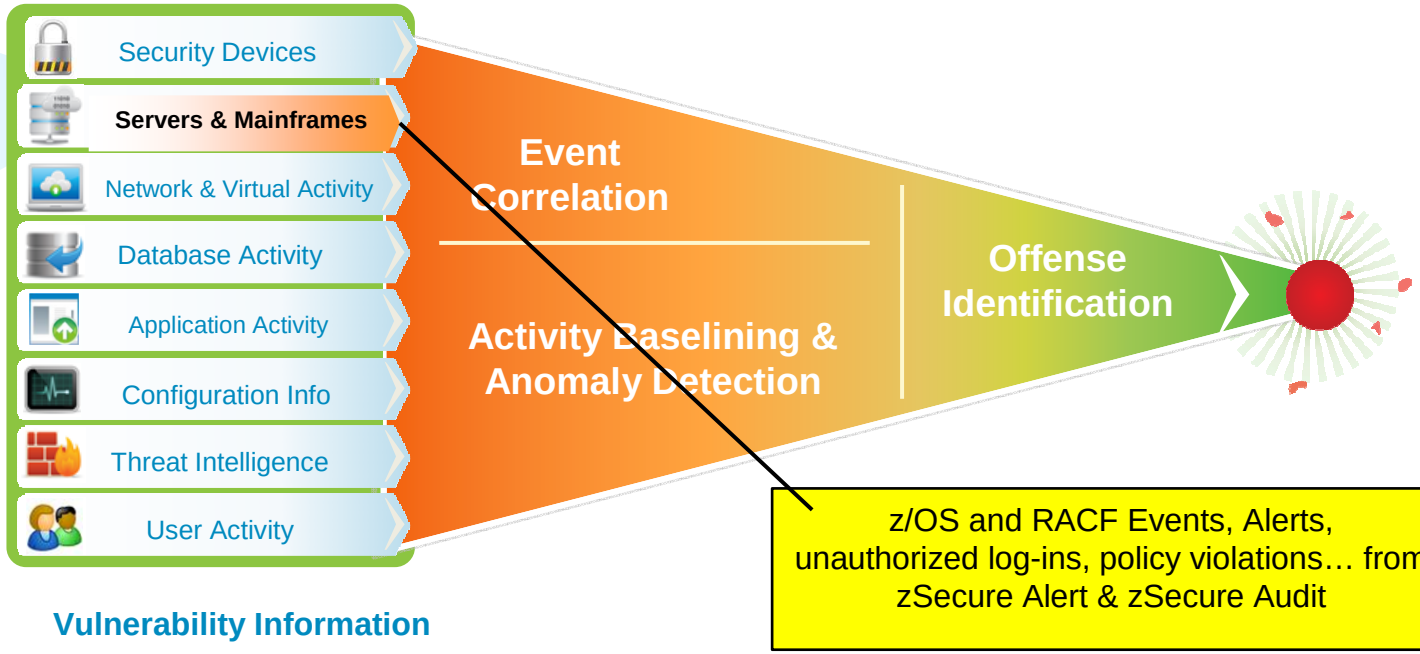


zSecure : simplifier, améliorer et renforcer la sécurité



Intégration de **zSecure** dans **QRadar**

- System z
- RACF
- ACF2
- Top Secret
- CICS
- DB2



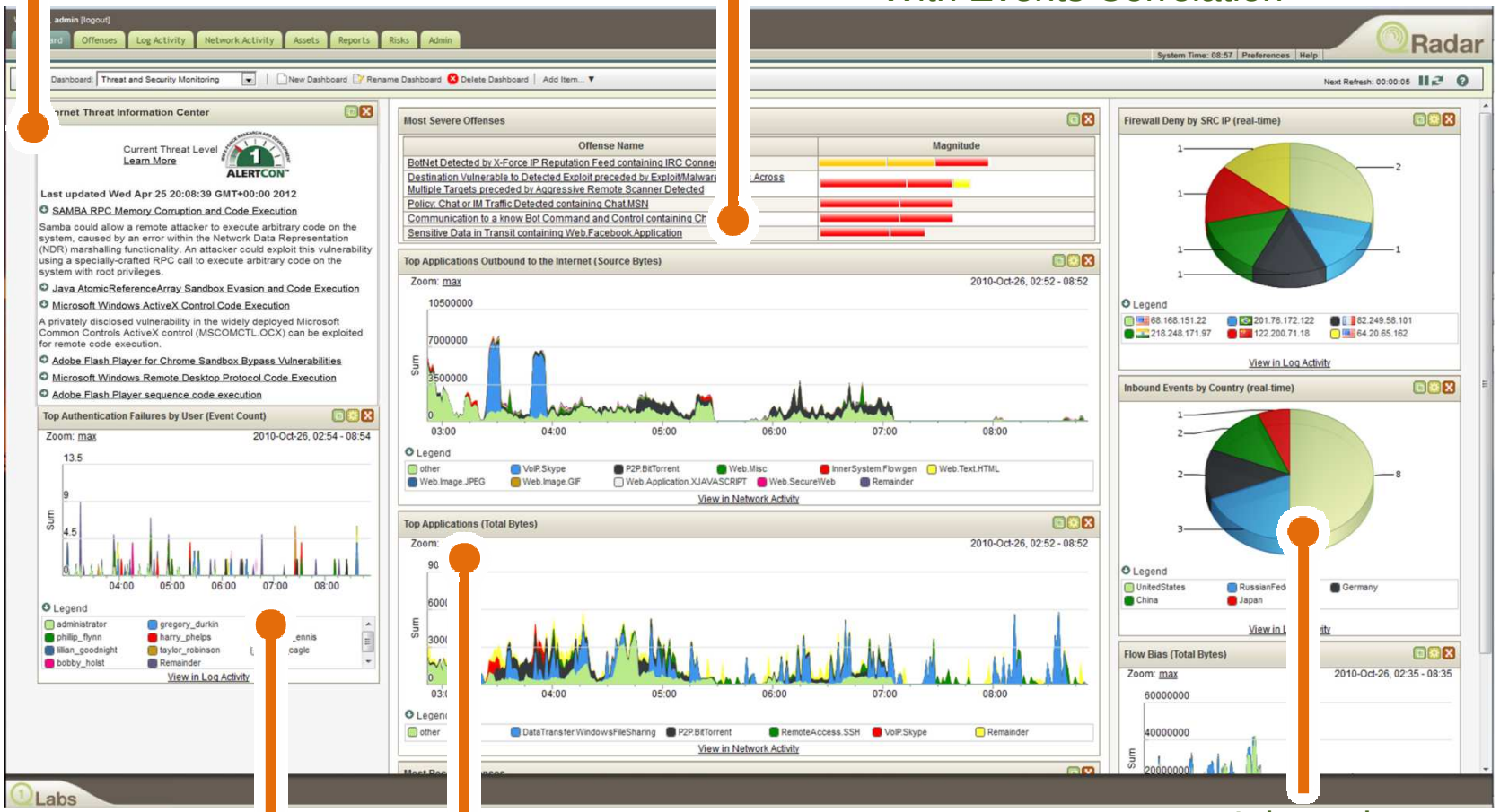
Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

- ✓ Vue centralisée du Mainframe et des systèmes distribués : incidents, activités, tendances
- ✓ Meilleure identification, priorisation et corrélation des menaces avec zSecure Alert
- ✓ Meilleure analyse des niveaux de risques et simplification des audits avec zSecure Audit

QRadar: Monitoring des événements multi-plateformes

IBM X-Force® Threat Information Center

Real-time Security Overview With Events Correlation



Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

Protection des données métiers

- Comment protéger et surveiller les accès aux données sensibles ?
  - Etablir une politique de sécurité
    - Qui a quel droit d'accès à quelle donnée ?
  - Créer, implémenter et valider cette politique dans RACF
  - Surveiller toutes les activités des utilisateurs

Protection des données sensibles dans les fichiers

- zSecure Admin : simplifier la gestion, l'analyse et les suivis
  - définir les niveaux de protection sur chaque fichier (Dataset Profile)
  - octroyer les droits d'accès aux Users via ACL (Access Controle List) sur ces « Datasets Profiles » définis selon la politique de sécurité.
  - surveiller en temps réel et à moindre coût, les activités de tous les utilisateurs : accès aux ressources (autorisés ou non)
  - analyser et supprimer des protections incohérentes ou obsolètes
- zSecure Audit et Alert : simplifier l'audit, la surveillance et les alertes
  - auditer la conformité des mesures de protection
  - détecter et être alerté en temps réel (zSecure Alert) ou en différé (zSecure Audit) des accès autorisés ou frauduleux sur ces fichiers.
  - prendre des mesures coercitives en temps réel (zSecure Alert) pour interdire aux utilisateurs de se connecter aux systèmes
  - envoyer ces événements d'accès « fichier » à un outil SIEM (Qradar)

Protection des données de Production

quand on les utilise dans d'autres environnements

Comment protéger contre les fuites de données sensibles dupliquées à partir de l'environnement de « Production » ?

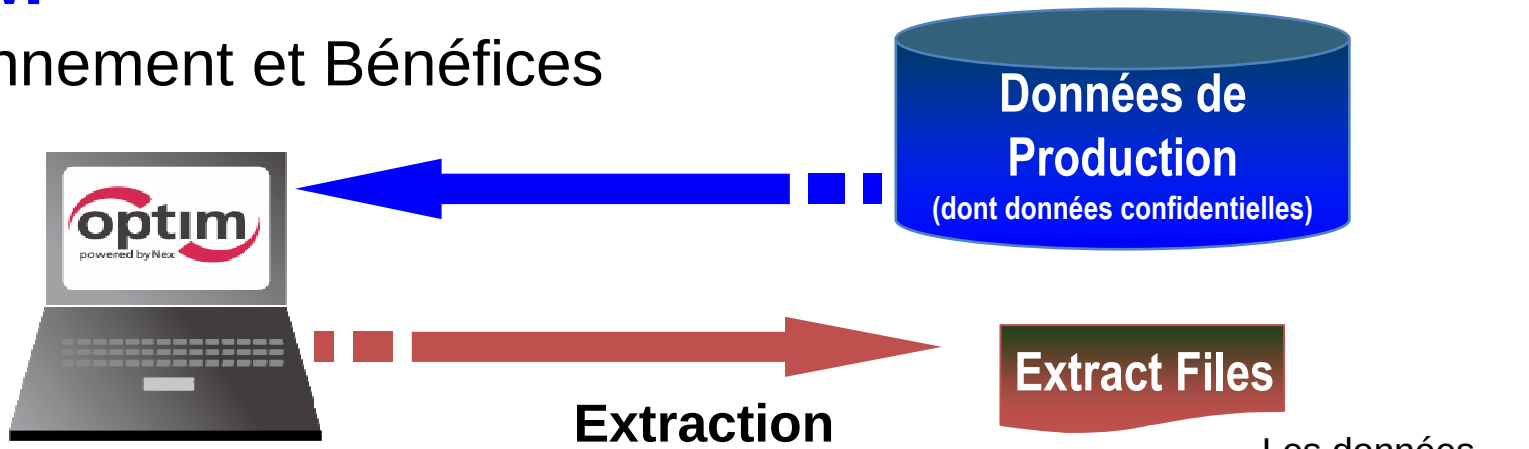
…c'est-à-dire dans le cadre de la création des jeux d'essai pour divers environnements : « Tests », « Intégration » ou « Recette » « Formation » ?

=> La solution **IBM OPTIM** facilite la création des jeux de tests en automatisant l'anonymisation des données sensibles de Production

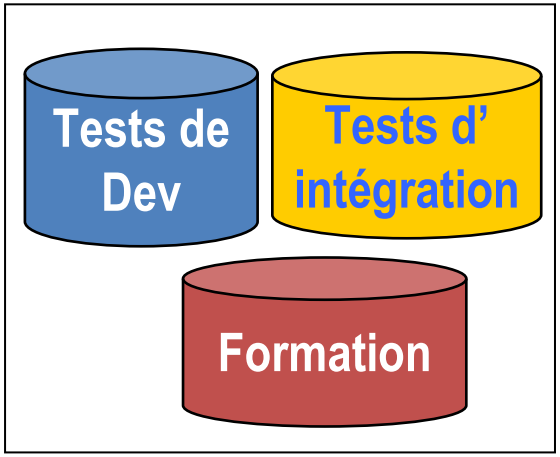
…/…

OPTIM –

Fonctionnement et Bénéfices



Les données confidentielles **sont maquillées avec des algorithmes personnalisables**



BENEFICES D'OPTIM :

- **Créer des environnements de données** à partir des données de production (ciblés, à leur juste taille, vite, à moindre coût)
- **Gérer la cohérence** entre les environnements de tests
- **Raccourcir le cycle des tests**.
- **Protéger les informations confidentielles** dans les environnements hors production

Protection des bases de données sensibles

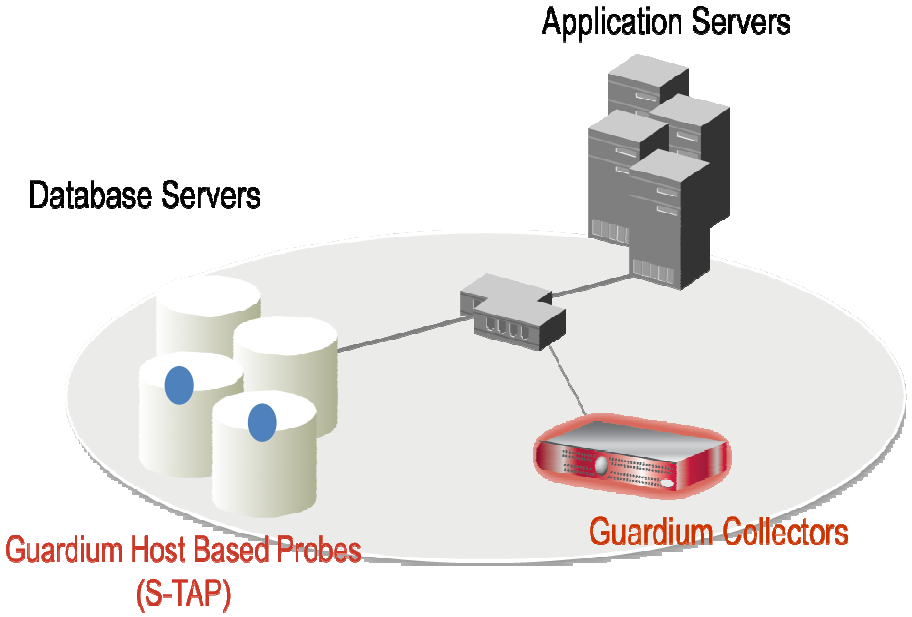
- Vous voulez savoir qui fait quoi, quand et comment sur vos données sensibles y compris dans un environnement hétérogène ?
- Vous voulez protéger les fuites d'informations ?

→ Solution : **InfoSphere Guardium Data Activity Monitor**

Problématiques de protection des bases de données

- Infrastructure hétérogène → Aucune méthode de sécurité et d'audit normalisée et unifiée
  - Bases de données: DB2, IMS, Oracle, MS SQL, DB2, Sybase, Informix, Netezza
  - Applications: CICS, IMS, SAP, Oracle EBS, Siebel, custom apps, etc.
  - Plate-formes : Windows, UNIX, Linux, z/OS
- Audit des bases de données fait avec des outils fournis par défaut
  - Logging, Traces, SQL traces, Audit natif des bases de données, etc…
- Impact sur les performances
  - Consommation significative de ressources CPU, car non conçu pour la sécurité
- Pas de protection en temps réel
  - Difficulté à créer des alertes sur des anomalies
  - Impossibilité de bloquer les activités non autorisées
- Pas de séparations des rôles
  - Les Utilisateurs privilégiés (DBA) ne doivent pas être leurs propres auditeurs

Guardium : Surveillance & sécurisation en temps réel



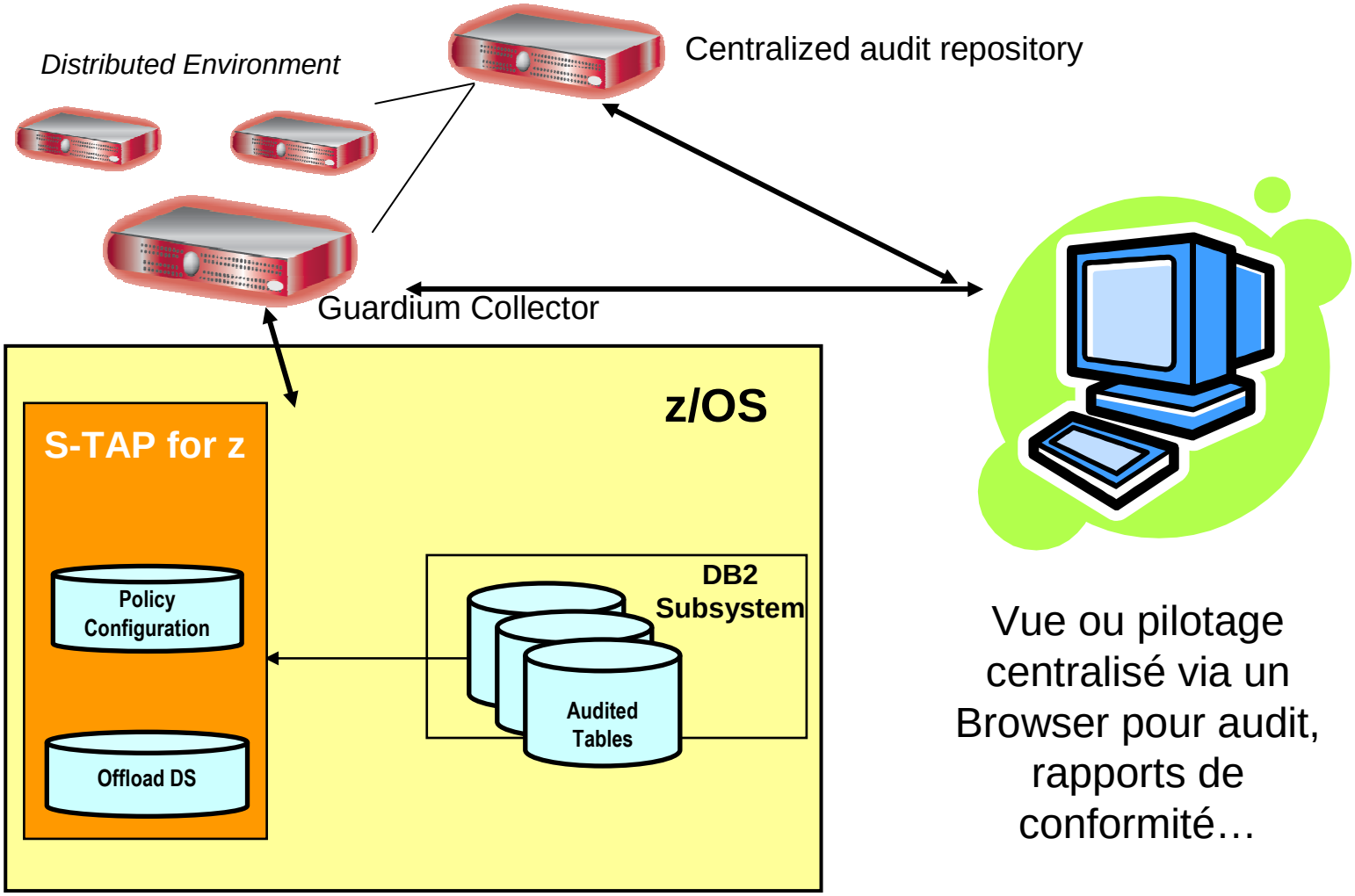
- Non-intrusif
- Nécessite aucun changement sur les Bases de données et applications
- Impact minimal
- Ne s'appuie pas sur les systèmes de log traditionnels de bases pouvant facilement être désactivés par les administrateurs

- Politiques granulaires & Surveillance
  - *Qui, Quoi, Quand, Comment*
- Alertes temps Réel
- Surveillance de toutes les activités utilisateurs privilégiés ou non
- Audit de vulnérabilités de bases de données

Plateformes supportées

Plateformes	Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gr2
Microsoft SQL Server / Microsoft SharePoint	2000, 2005, 2008 / 2007, 2010
IBM DB2 UDB (Linux, Unix, Linux for z)	9.1, 9.5, 9.7
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM DB2 UDB for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10, 11
IBM Netezza	4.5, 4.6, 5.0, 6.0
IBM IMS Database	9, 10, 11, 12
IBM VSAM Datasets	z/OS (toutes versions)
IBM DB2 UDB (Windows)	9.1, 9.5, 9.7
Sybase IQ	12.6, 12.7, 15
Sybase ASE	12, 15, 15,5
MySQL (Sun)	4.1, 5.0, 5.1
Teradata	6.01, 6.02, 12, 13, 13.10
PostgreSQL	8.9

InfoSphere Guardium for z – Architecture

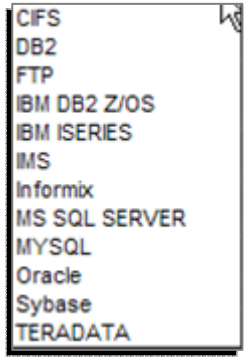


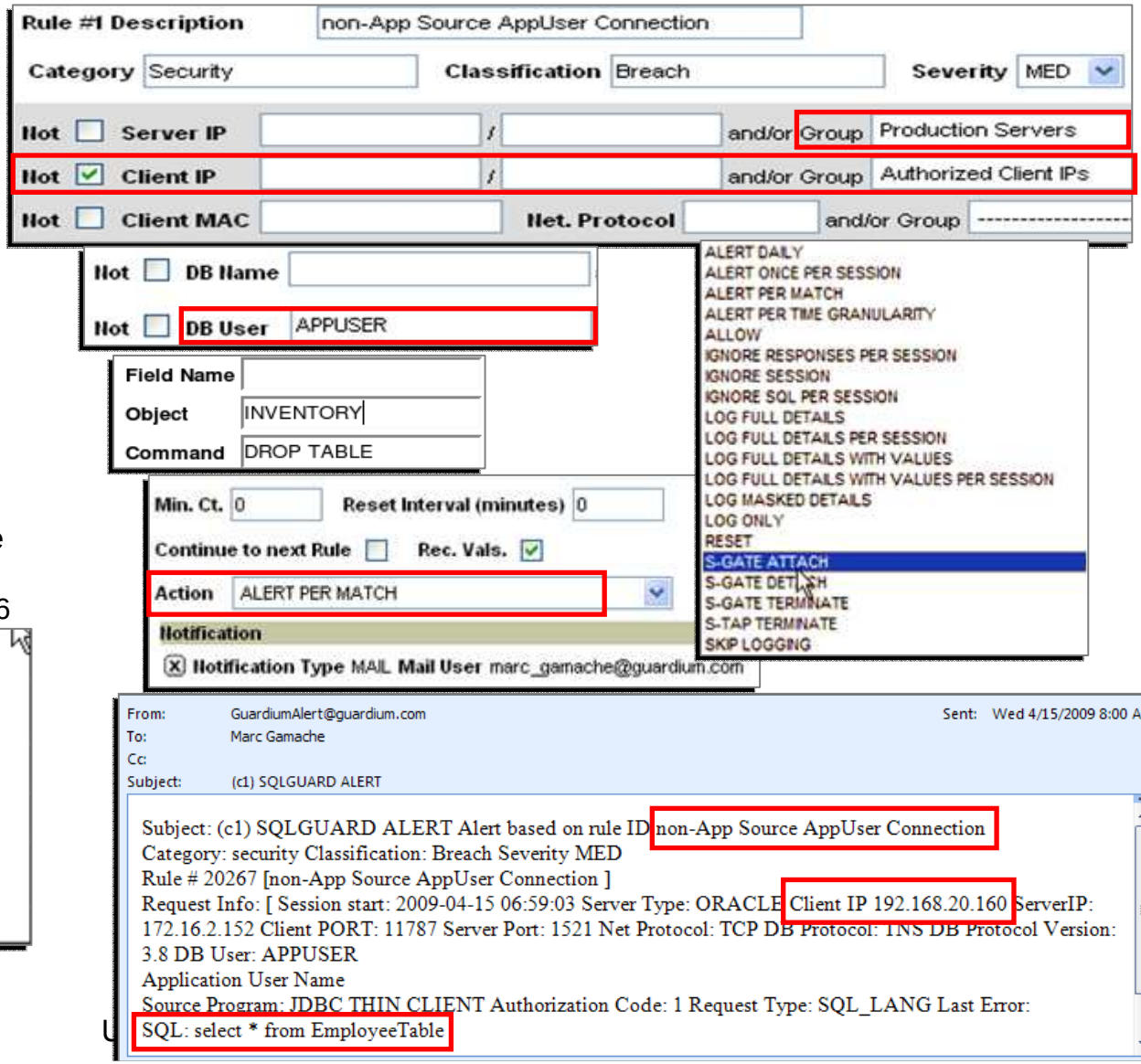
Vue ou pilotage centralisé via un Browser pour audit, rapports de conformité…

Règles de détection avec alertes en temps réel

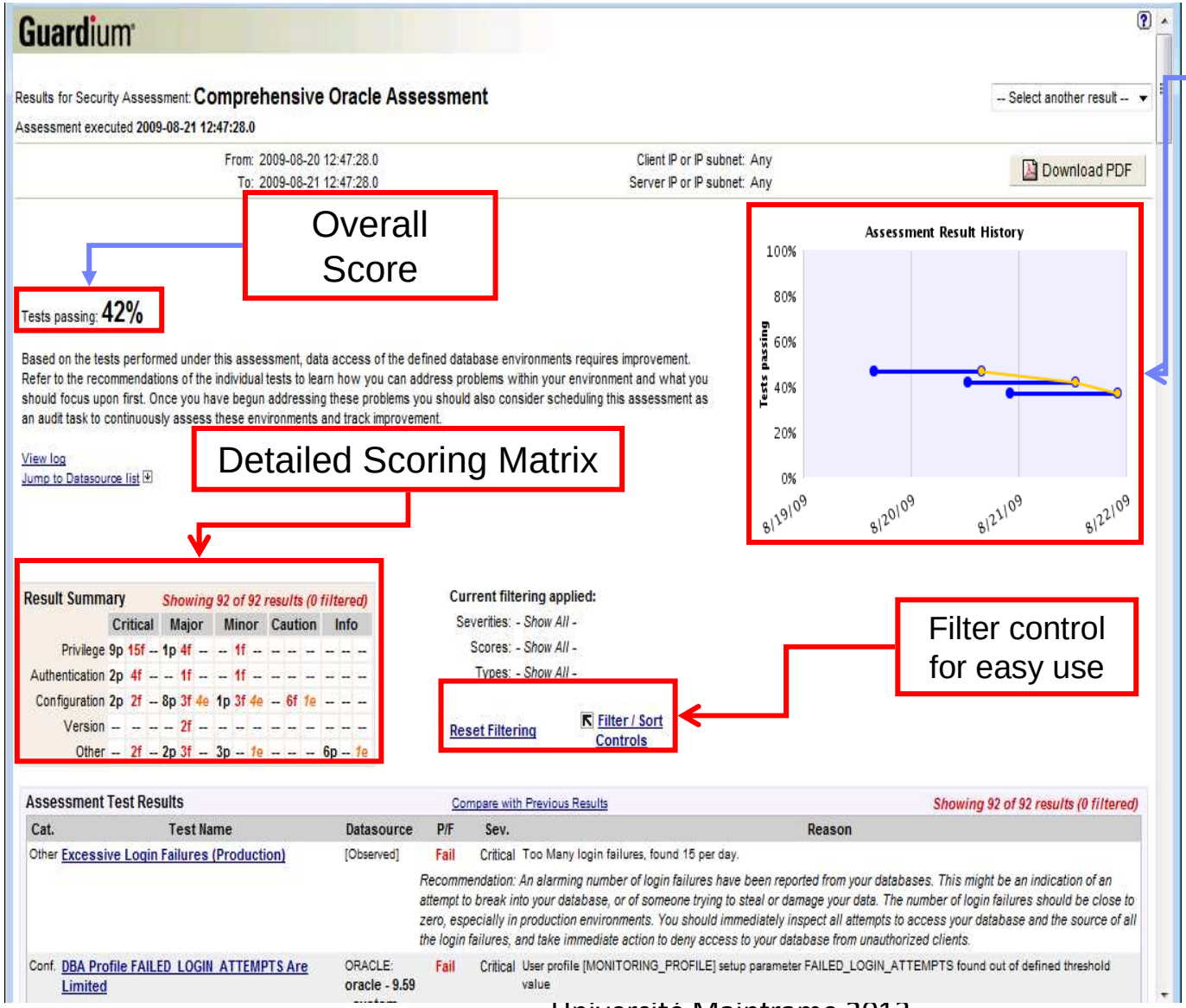
Application Server 10.10.9.244

Database Server 10.10.9.56

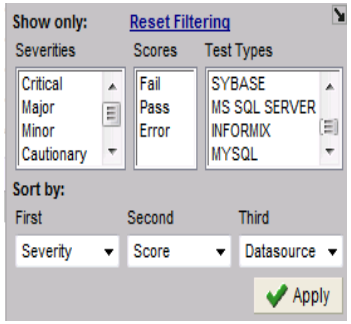




Guardium Assessment Results



Historical Progress or Regression



Chiffrement (Data encryption)

- Chiffrer les données sensibles afin de se conformer aux exigences réglementaires (ex : PCI DSS)

→ Data Encryption Tool for DB2 & IMS

Objectifs :

- Chiffrer les données sur disque pour rendre les accès directs inexploitables, c'est-à-dire hors DB2 et/ou IMS.

- Empêcher la fuite des données en clair

- Solution complémentaire avec Guardium pour z/OS

InfoSphere Guardium Data Encryption for DB2 & IMS

Installation transparente et rapide

Aucun changement aux applications, aux bases de données sous-jacentes ou à l'infrastructure matérielle.

Gestion centralisée des clés et des politiques

Accès à un système de gestion unifiée afin de simplifier la gestion de la sécurité des données.

Fonctions optimisées pour la conformité (PCI-DSS)

Vérification et production de rapports granulaires qui aident les utilisateurs à se conformer aux exigences en matière de gouvernance de données

Outil unique pour sécuriser des bases de données DB2 et IMS

Requirements

- Protect sensitive enterprise information and avoid production data breaches
- Centralized policy and key management
- Protect data on portable media and render it unusable if stolen or lost

Benefits

- Comply with government and industry regulations (for eg. PCI-DSS)
- Reduce internal and external risk and threat exposure
- Minimize impact on applications

Webographies

IBM Security zSecure v1.13 Announcement Information

- http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc_1.13/welcom.htm

zSecure data sheets, solution sheets, and white papers

- http://www-306.ibm.com/software/tivoli/products/zsecure/

zSecure Manuals

- http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc/welcome.htm

InfoSphere Guardium Data Security Library

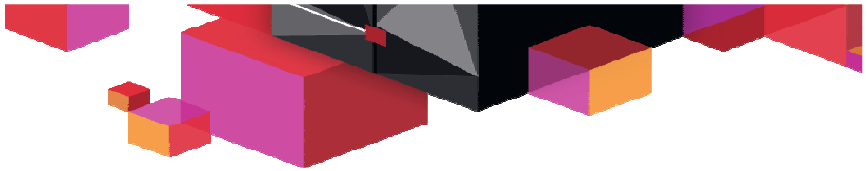
- http://www-01.ibm.com/software/data/guardium/library.html

InfoSphere Guardium Data Encryption for DB2 and IMS Databases

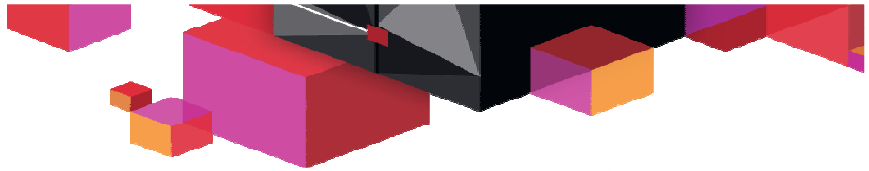
- http://www-01.ibm.com/software/data/db2imstools/db2tools/ibmencrypt/

Redbooks

- http://www.redbooks.ibm.com/



Questions



धन्यवाद

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

Thank You

English

شكرا

Arabic

Obrigado

Brazilian Portuguese

Danke

German

Grazie

Italian

多谢

Simplified Chinese

Merci

French

நன்றி

Tamil

ありがとうございました

Japanese

감사합니다

Korean