Expert de la sécurité des SI

Traçabilité / Conformité/ Protection

Le tryptique de Guardium

MENSAH Luc

Dir. Technique NSIT

CISSP, CEH, ISO 27001 & 27005

MONTRI Stéphane

Responsable offre Gouvernance, IBM

Août 2013

Les thèmes

Observations de portée générale

- la vision de la sécurité / Le Positionnement du Produit
- Le contexte: la valorisation exponentielle de l'actif immatériel
- Les menaces, les obligations, les risques
- le constat

- **Guardium dans l'Entreprise**
  - Le positionnement dans l'organisation l'Entreprise
  - les problèmes à résoudre

Guardium V9: une brève présentation

- Fonctionnalités, couverture
- Intégration dans l'Entreprise

Positionnement du Produit…

- …Dans une perspective d'évolution des tendances de la sécurisation:
  - Sécurisation périmétrique: pare-feu stateful, Reverse Proxy niveau 7,
  - Du réseau: IDS/IPS
  - Protection applicative: WAF,
  - Du serveur, poste de travail: AV, contrôle de conformité

Aujourd'hui,

protection des silos de données **abstraction faite des moyens** et technologies **d'accès**

Le contexte : l'information est un actif clé dans l'entreprise

- Les données les plus précieuses
  - Données financières, comptables (prêts, virements, …)
  - Informations métier (contrats, brevets, code…)
  - Informations d'identification personnelle (banques, hôpitaux, administrations)

- Disponibilité d'importants volumes de données structurées

- Multiples accès à l'information

… qui - comme tout actif - doit être protégé des risques potentiels et respecter la règlementation auxquels il est soumis…

3 catégories principales de risques

1. **Menaces internes**
   - Changements non autorisés (gouvernance)
   - Fuites d'information
2. **Menaces externes**
   - Vol,
   - Corruption de données
3. **Conformité**
   - Complexité des processus
   - Élévation des coûts des contrôles

… tout en prenant en compte le renforcement des contraintes imposées par le marché ou les régulateurs

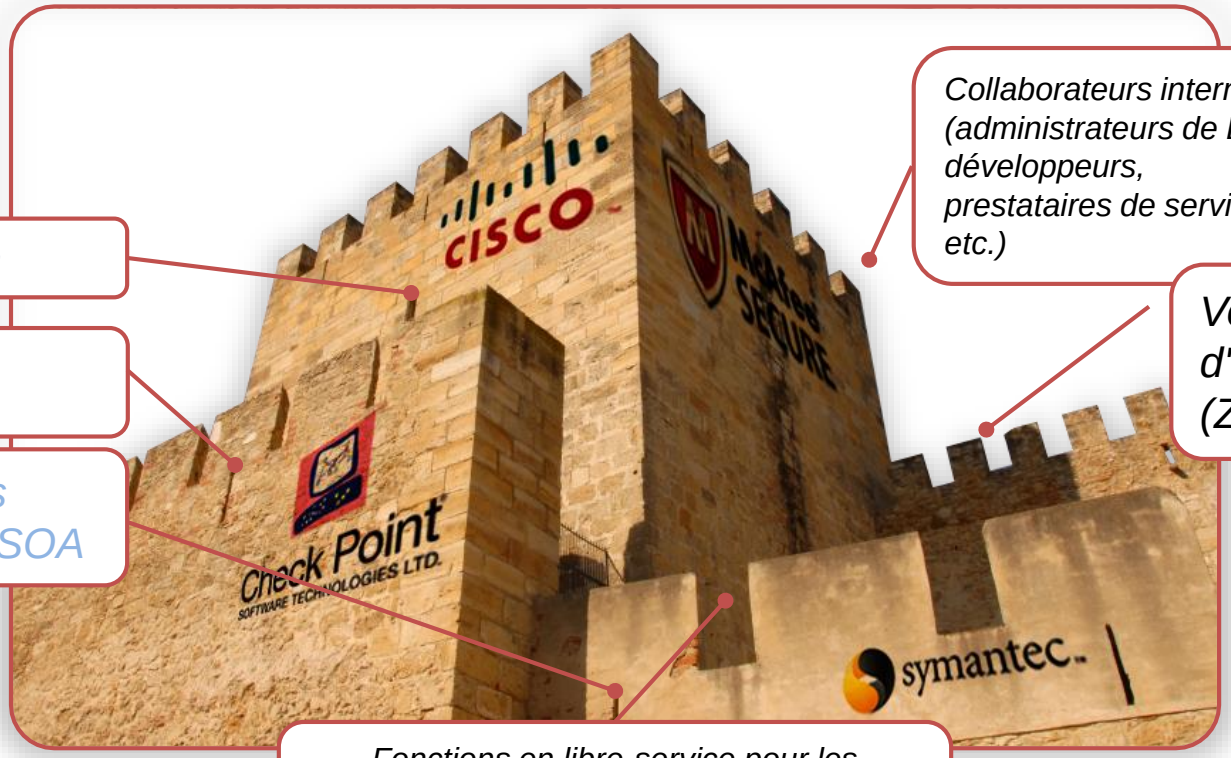
- L'explosion des violations réussies a entraîné une réglementation plus stricte des données sensibles en Amérique du Nord
  - SOX
  - HIPAA
  - PCI DSS
  - 46 lois étatiques relatives à la confidentialité des données
  - Gramm-Leach-Bliley
- De nombreux pays d'Europe et d'Asie ont déployé des réglementations similaires
  - Directive européenne sur la confidentialité des données et législations locales sous-jacentes
  - C-SOX
  - FIEL
  - PCI DSS
  - LCEN
  - etc.

Constat

Les défenses périmétriques ne suffisent plus

« L'approche de type forteresse ne fonctionne pas dans le cyberespace. Il n'est plus possible de se retrancher derrière une ligne Maginot de pare-feu. »

- William J. Lynn III,
  Secrétaire adjoint à la défense américaine



Externalisation

"WebFacing" des applications

Intégration des applis natives/SOA

Collaborateurs internes (administrateurs de BD, développeurs, prestataires de services, etc.)

Vol d'informations d'identification (Zeus, etc.)

Fonctions en libre-service pour les employés ; partenaires et fournisseurs

Dans l'Entreprise: le(s) bénéficiaire(s) potentiel(s) de Guardium

- Le métier:
  - Traçabilité,
  - Protection des bases de données,
  - Homogénéité de la solution (agnostique du type de Base de Données)

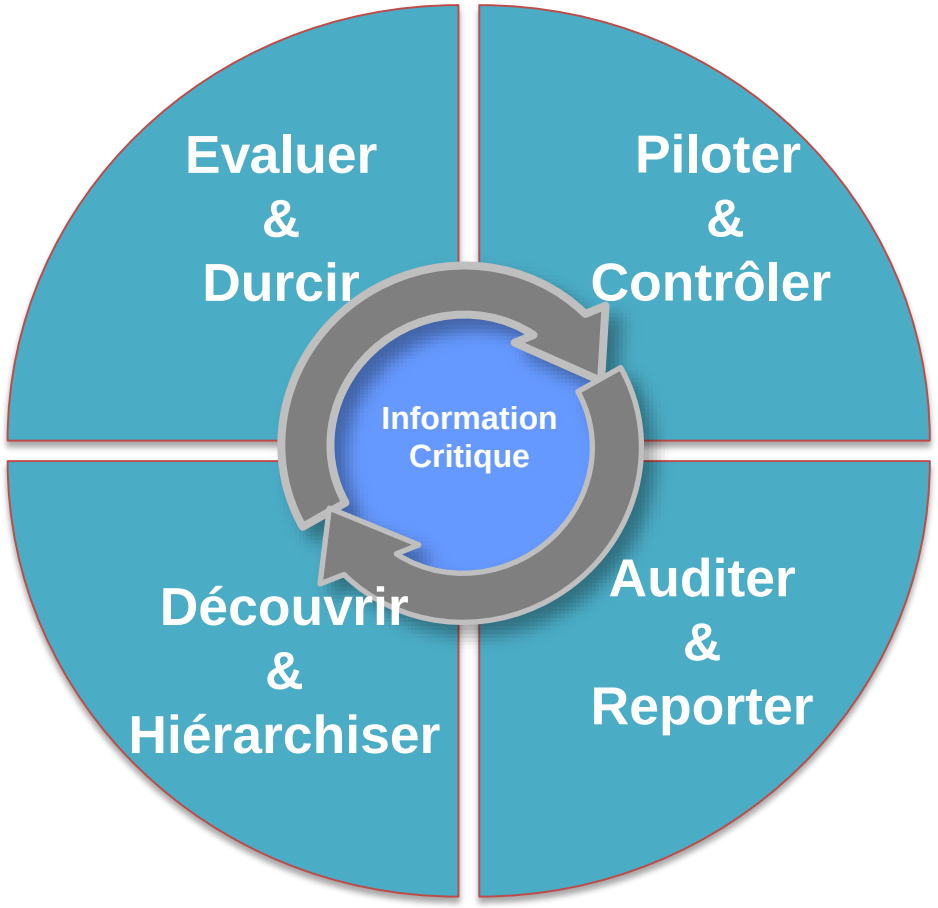
- Le RSSI (régulation)
  - Atteinte à, et preuve de, la Conformité,
  - Les rapports à vocation managériale, du contrôle interne

- Les opérationnels (bases de Données, sécurité)
  - Application opérationnelle sur les données de la PSSI…

Pour protéger ces données, l'entreprise doit être capable de répondre aux questions :

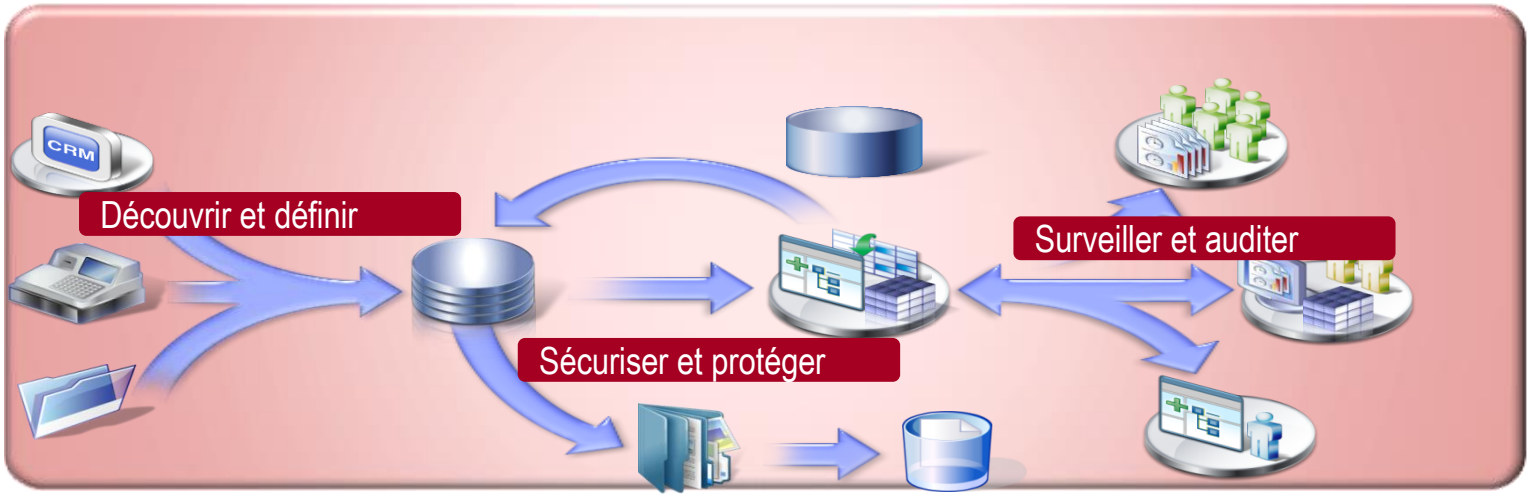
- Où sont situées mes données sensibles et qui y accède ?
- Comment puis je renforcer l'accès à mes données et garder un œil sur la modification des politiques d'accès ?
- Comment auditer les vulnérabilités d'accès à mes données et superviser les changements de configurations ?
- Comment puis je simplifier et automatiser la mise en conformité des règles d'accès en usage dans le périmètre dont j'ai la charge ?

Dans l'objectif de couvrir tous les cycles de la sécurité et de la conformité …

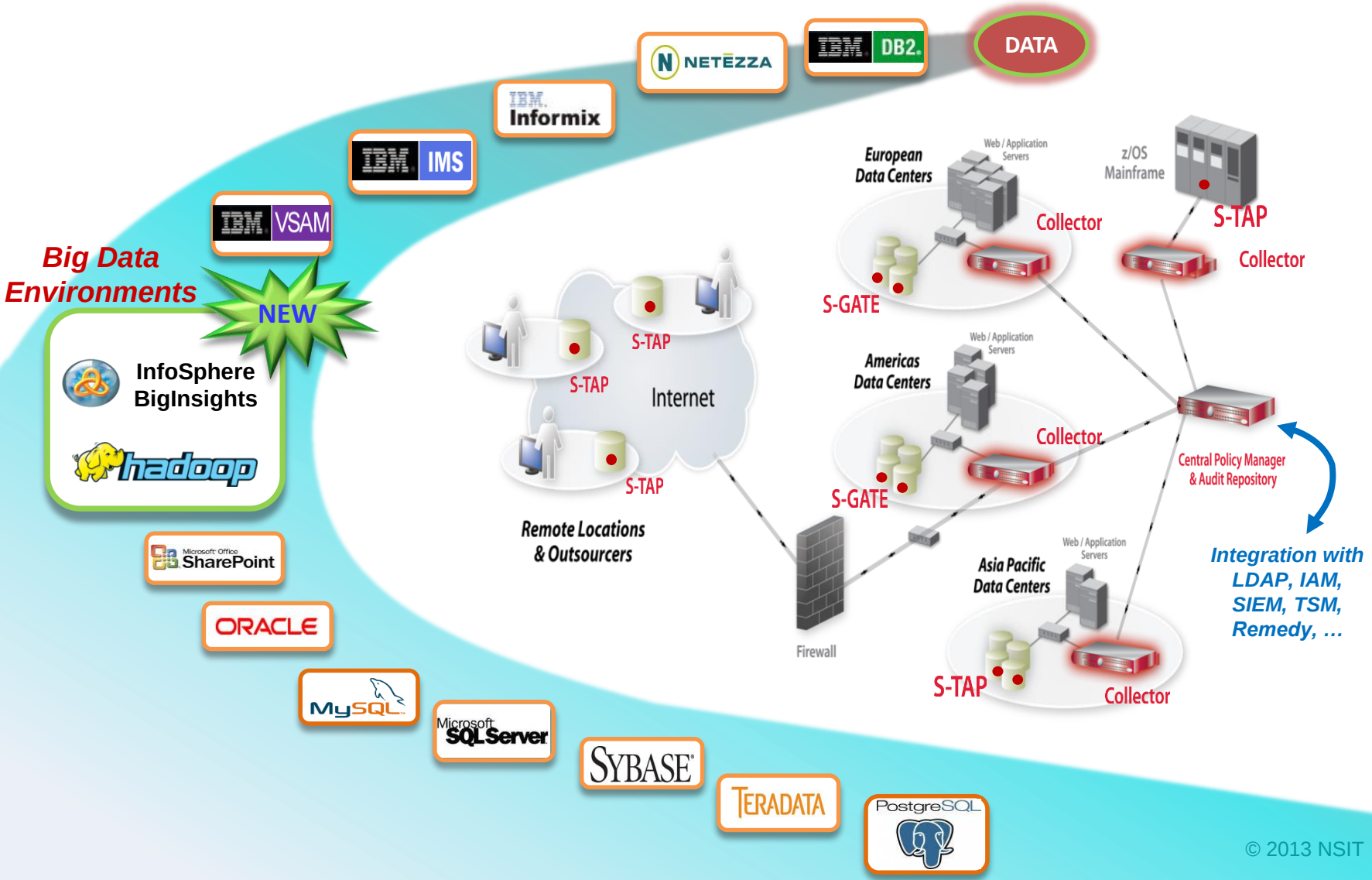


Et pour savoir quels sont les critères pertinents du choix d'implantation d'une solution:

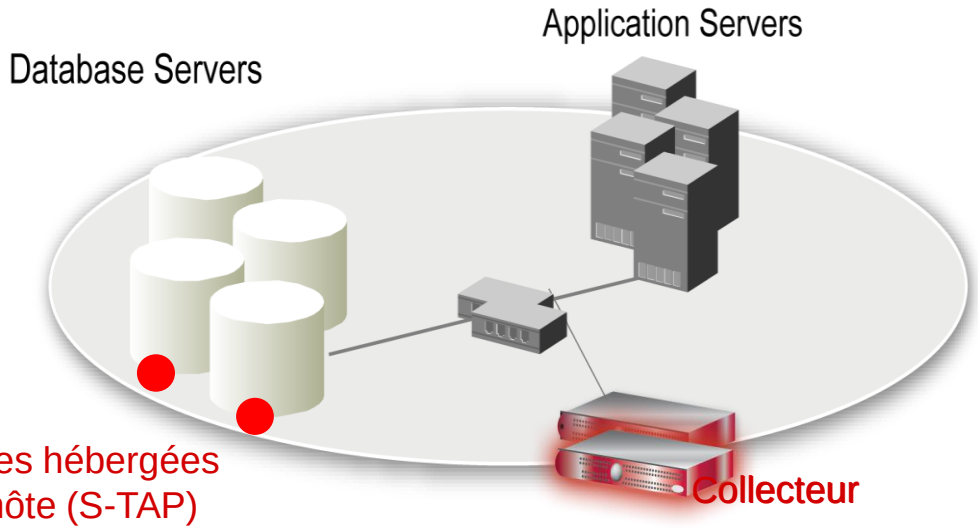
- Connaître les composantes « Quoi » et « Où » des données d'entreprise
- Protéger les données à l'échelle de toute l'entreprise, tant contre les menaces externes qu'internes
- Savoir qui accède à vos données, quand, comment et dans quel but
- Surveiller et générer des rapports sur l'accès aux données, à des fins d'audit



Combine la traçabilité et le contrôle de traffic avec la protection des données sensibles hébergées dans les “data warehouses”



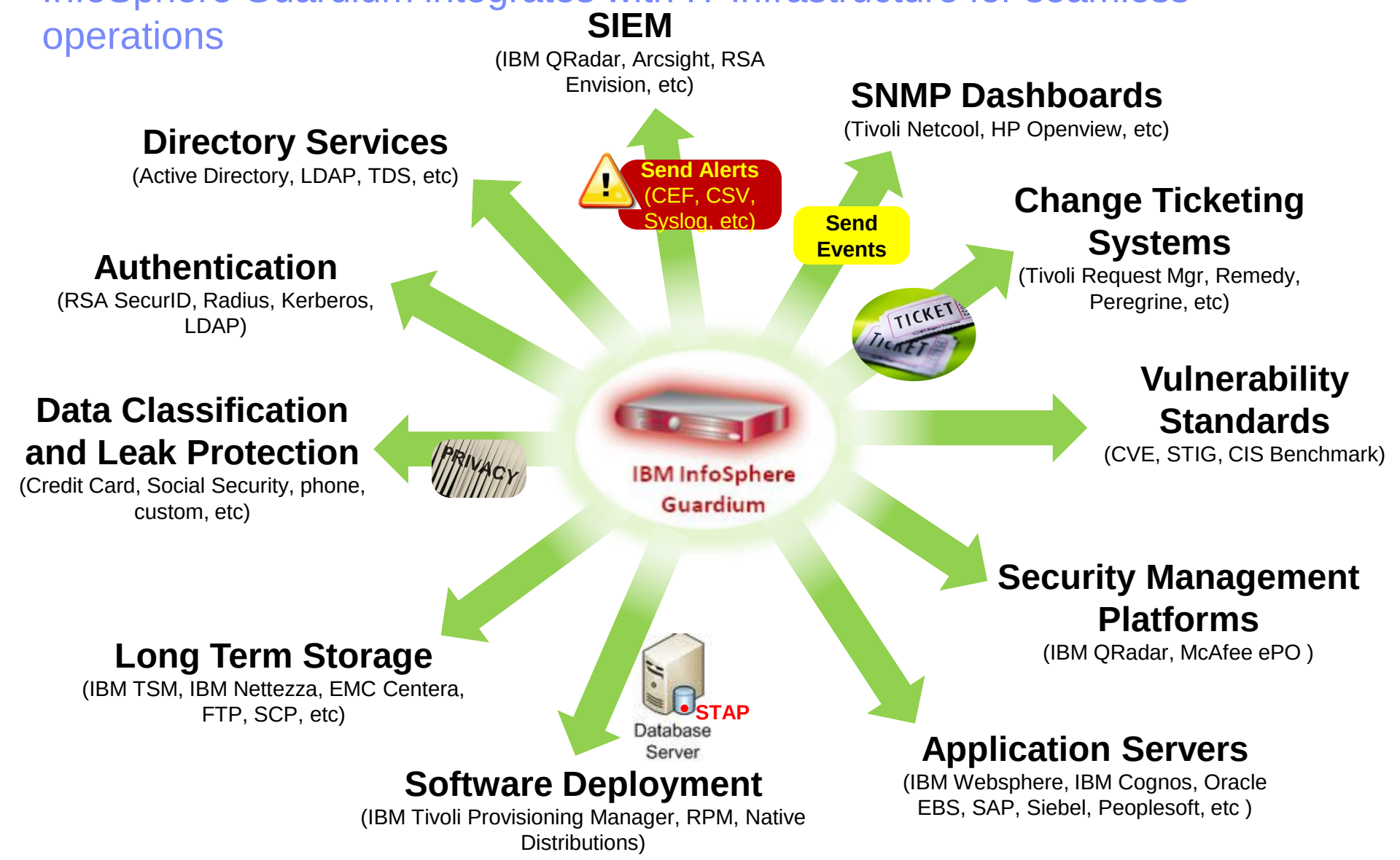
Surveillance de bases de données en temps réel



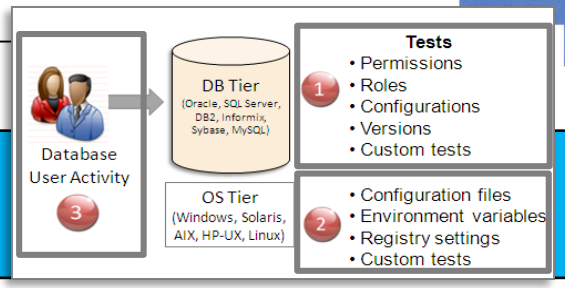
- Architecture non invasive
  - Extérieure à la base de données
  - Répercussions minimes sur les performances (2-3 %)
  - Aucune modification sur le SGBD ou les applications
- Solution compatible multi-SGBD
- Visibilité intégrale, y compris sur les accès des administrateurs de bases de données

- Assure la séparation des tâches
- Ne s'appuie pas sur des fichiers journaux rattachés au SGBD, qui peuvent être aisément effacés par les pirates ou des collaborateurs internes malintentionnés
- Politiques et audits granulaires, en temps réel
  - *Qui, quoi, quand, comment*
- Génération automatisée de rapports de conformité, des approbations et des escalades (SOX, PCI, NIST, etc.)

InfoSphere Guardium integrates with IT Infrastructure for seamless operations

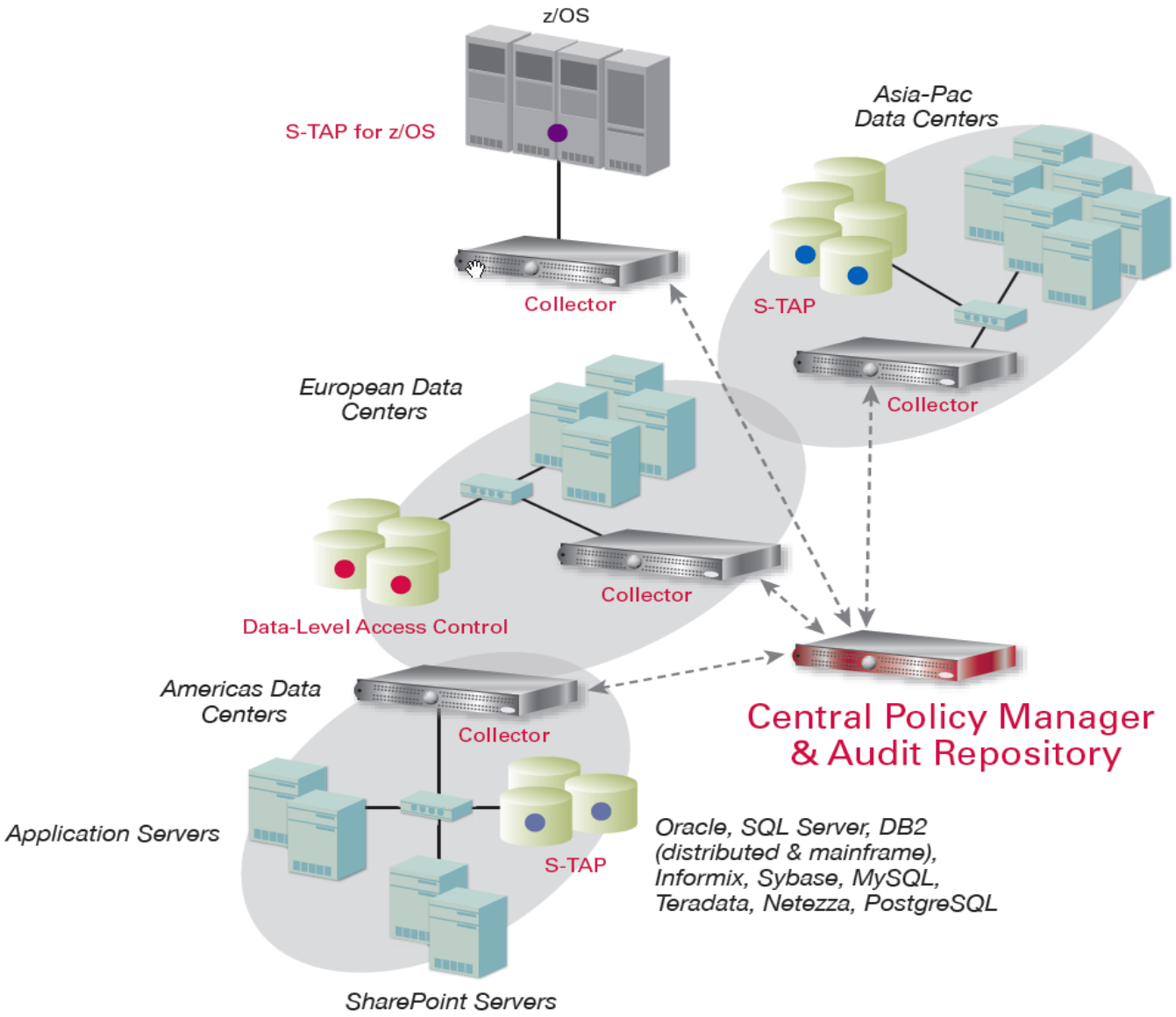


Politiques basées sur les normes de l'industrie



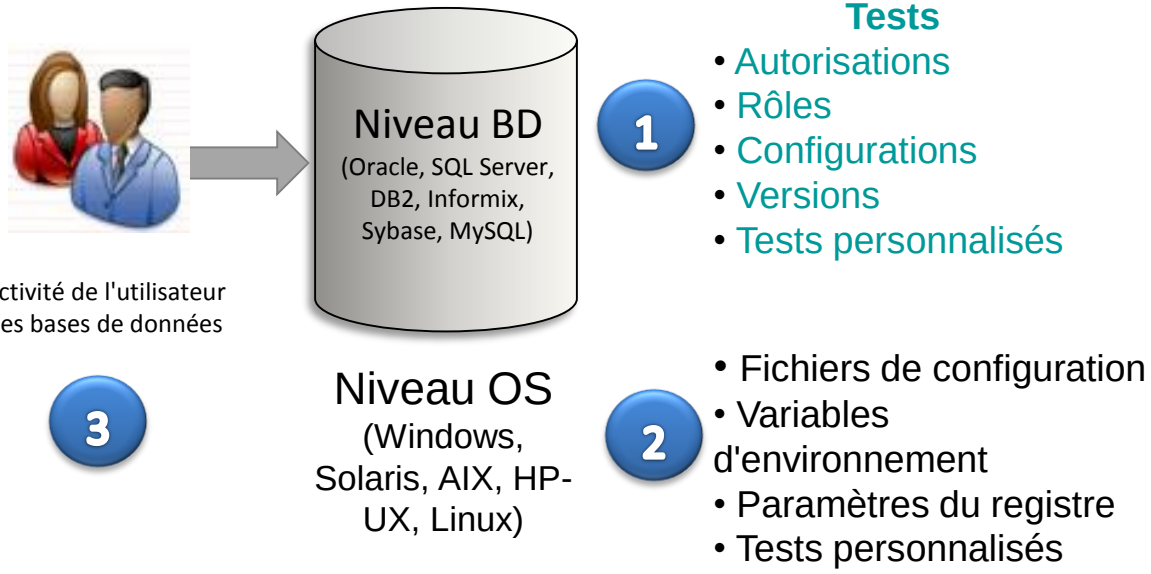
Section STIG	Exigence STIG	Section CIS		Surveillance par Guardium
2 : Intégrité du SGBD	Surveiller les versions actuelles et le niveau des correctifs installés, les changements non autorisés, les droits d'accès aux systèmes de production accordés aux développeurs, les requêtes ponctuelles.	2,12 : Oracle 2: SQL Server	Installation et niveau des correctifs installés, création d'objets pour les changements non autorisés, surveiller l'accès des développeurs aux systèmes de production, éviter les requêtes ponctuelles sur les bases de données de production, appliquer un processus de contrôle des changements.	✓
3 : Contrôle des accès	Traçabilité de toutes les actions pour remonter jusqu'à l'utilisateur qui en est à l'origine, concept des droits d'accès minimaux (utilisateurs, rôles et comptes), pas de comptes partagés, pas de comptes par défaut, verrouillage des comptes après 3 échecs de connexion, force minimale des mots de passe, changement des mots de passe tous les 90 jours, restriction des accès via les comptes de service partagés (pools de connexions), validation de tous les comptes des administrateurs de bases de données par le responsable de la sécurité des informations (IAO).	2, 11 : Oracle 1, 3, 4, 6, 8 : SQL Server	pas de comptes par défaut, définition de mots de passe, blindage des bases de données, comptes invités désactivés, multiples procédures de stockage étendues désactivées, mots de passe forts pour les connexions SQL, attribution d'autorisation pour les rôles autres que les utilisateurs, analyse périodique des rôles.	✓
4 : Audit de bases de données	Auditer toutes les opérations sur base de données avec une granularité suffisante pour détecter les activités d'intrusion, surveiller toutes les connexions des administrateurs de bases de données, s'assurer que les données d'audit ne soient consultables que par le personnel autorisé, absence d'applications non autorisées ou de lots de travaux, détecter les modèles d'activité inhabituels ou suspects, surveiller les changements apportés aux objets des bases de données, analyser quotidiennement les données d'audit, conserver les données d'audit pendant 1 an.	12 : Oracle 4, 5 : SQL Server	Vérifier les personnes rattachées au groupe des administrateurs de bases de données, analyser et contrôler les applications accédant aux bases de données, analyser régulièrement les données d'audit, auditer l'activité des utilisateurs habilités (accès aux objets, processus gérés, ajout d'utilisateurs des bases de données, etc.).	✓
5 : Accès réseau	Cryptage (et surveillance) des connexions distantes des administrateurs, identification des utilisateurs des bases de données passant par un pool de connexions, comptes de base de données distincts pour la réplication, éviter que les développeurs n'accèdent à des données sensibles.	12 : Oracle 1, 2 : SQL Server	Cryptage, modification des ports par défaut pour SQL Server.	✓
6: Autorisations de l'OS	Vérifier les autorisations de fichier pour les exécutables des bases de données, les fichiers de configuration et les fichiers de données, s'assurer que seuls les administrateurs de bases de données autorisés deviennent membres des groupes de système d'exploitation bénéficiant de droits d'accès supérieurs au SGBD.	1 : Oracle 1, 3 : SQL Server	Registre Windows, refuser le groupe de système d'exploitation correspondant aux Invités, configuration de référence du système d'exploitation.	✓

Architecture évolutive multiniveau

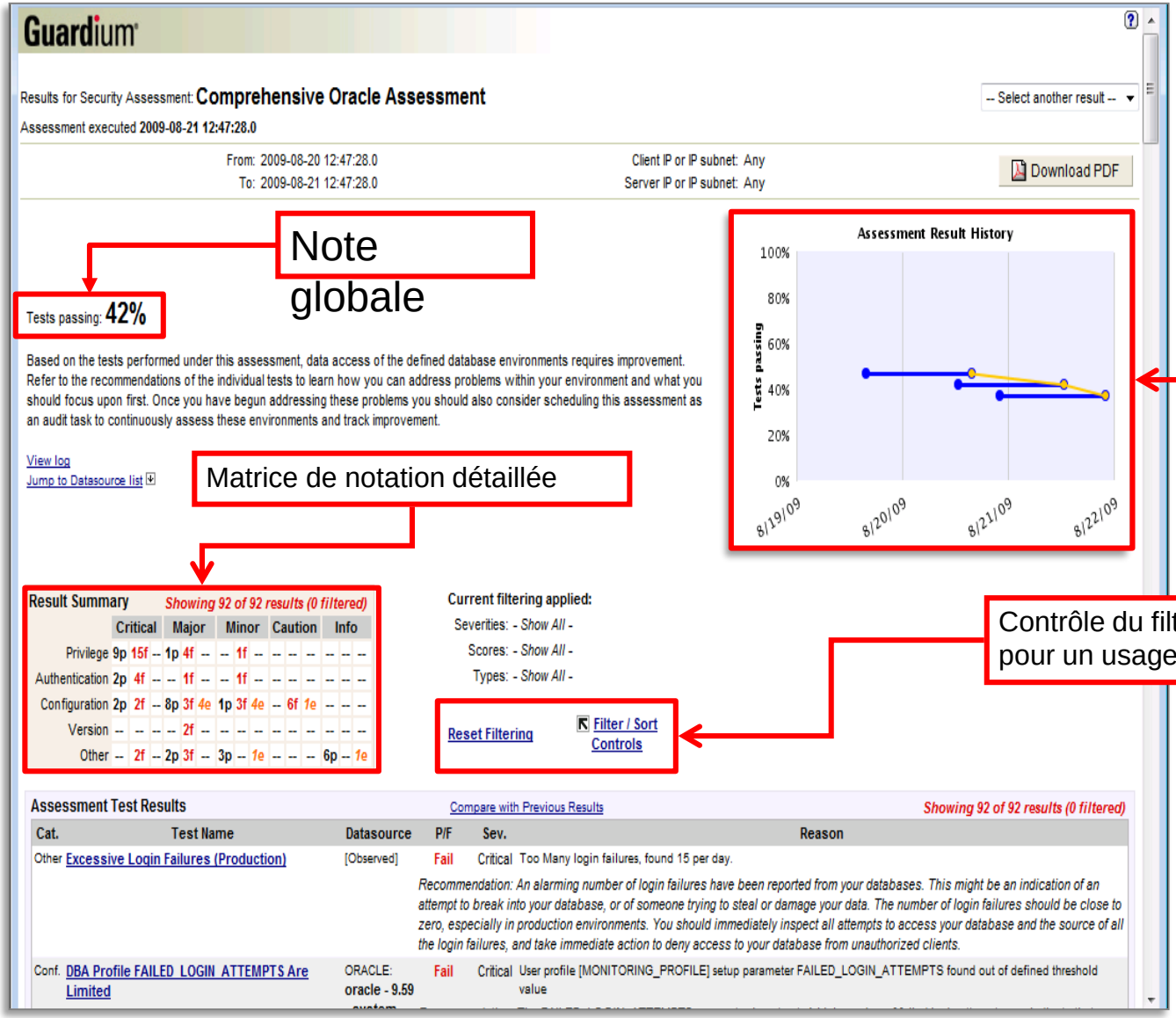


Détection des vulnérabilités et évaluation de la configuration

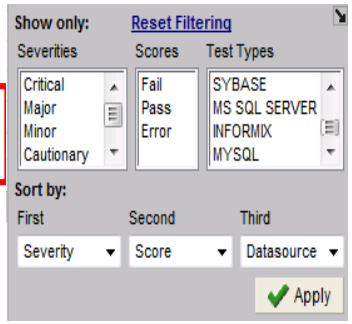
- S'appuie sur des normes de l'industrie (DISA STIG et benchmark CIS)
- Personnalisable
  - Via des scripts personnalisés, des requêtes SQL, des variables d'environnement, etc.
- Série de tests garantissant une couverture exhaustive :
  - Paramètres des bases de données
  - Système d'exploitation
  - Comportement observé



Exemple de détection de vulnérabilités



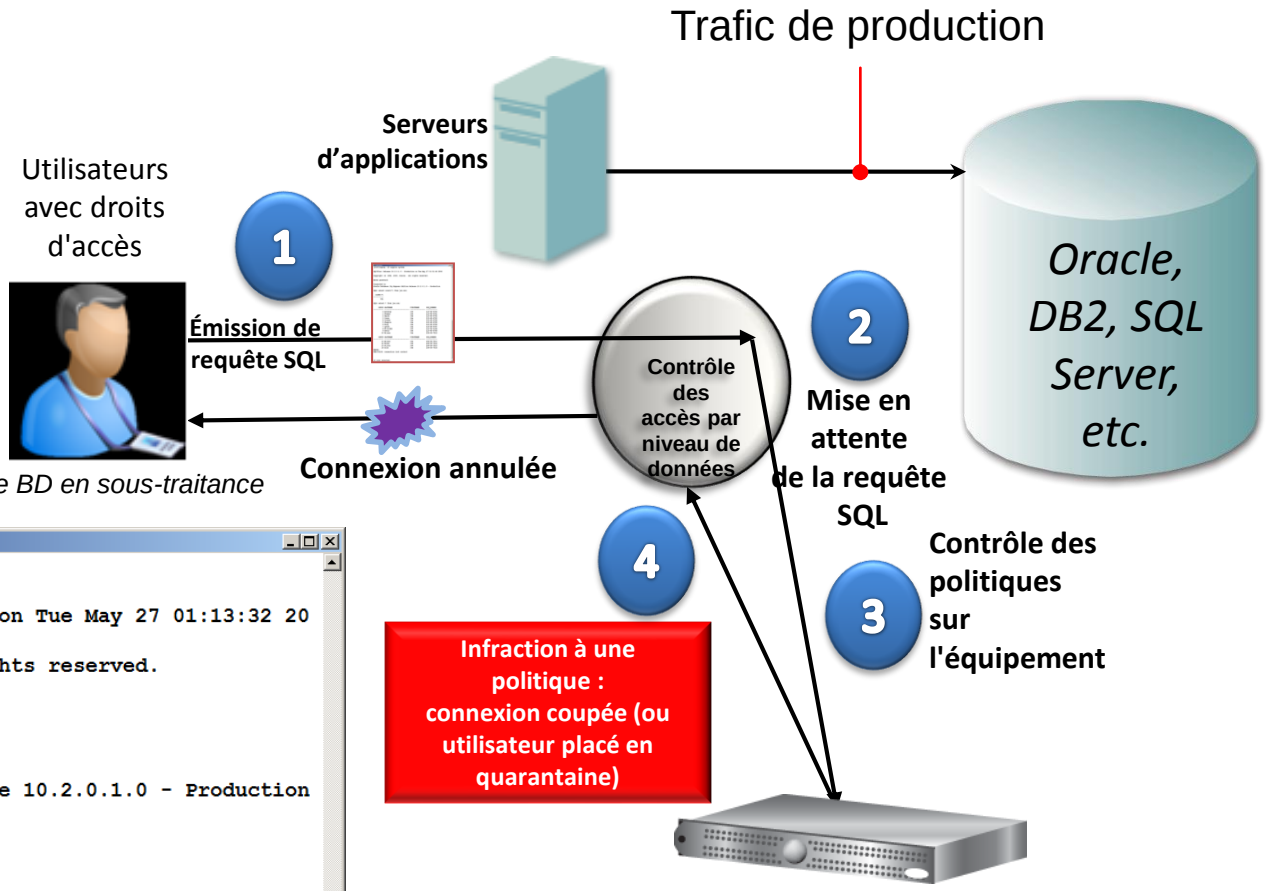
Historique indiquant une progression ou une régression



Contrôle du filtrage pour un usage aisé

Contrôle des accès par niveau de données : assurer un blocage sans équipements en ligne

« Les SGBD ne protègent pas les données contre les administrateurs. Ceux-ci peuvent donc aujourd'hui consulter ou dérober des données confidentielles stockées dans une base de données. » Cabinet Forrester, « Database Security: Market Overview », Fév. 2009

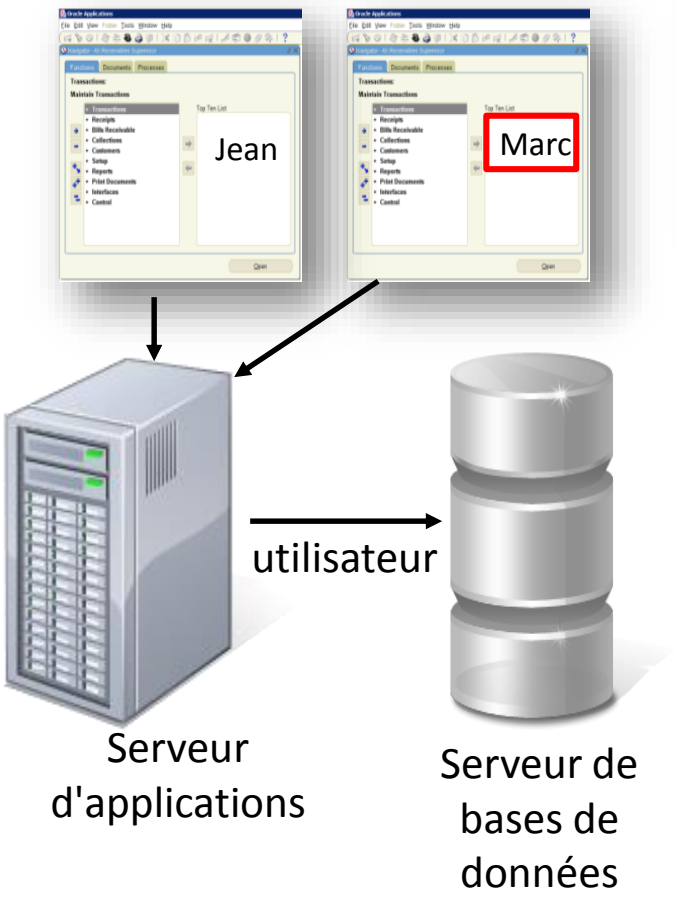


Ex: Administrateur de BD en sous-traitance

```
root@osprey:~
[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 clôturée

Identification des fraudes au niveau de la couche Application



DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***Problème*** : le serveur d'applications utilise un compte de service générique pour accéder à la base de données
  - La personne ayant initié la transaction ***n'est pas identifiée*** (pools de connexions)
- ***Solution*** : Guardium assure le suivi des accès des ***utilisateurs des applications, en se basant sur des commandes SQL spécifiques***
  - Prise en charge en standard de toutes les grandes applications d'entreprise (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) et des applications personnalisées (WebSphere...)

Des politiques affinées avec des alertes en temps réel

Serveur d'application
10.10.9.244

Serveur de bases de données
10.10.9.56

CIFS
DB2
FTP
IBM DB2 Z/OS
IBM ISERIES
IMS
Informix
MS SQL SERVER
MYSQL
Oracle
Sybase
TERADATA

Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

Not ☐ Server IP / and/or Group: Production Servers

Not ☑ Client IP / and/or Group: Authorized Client IPs

Not ☐ Client MAC | Net. Protocol | and/or Group

Not ☐ DB Name

Not ☐ DB User: APPUSER

Field Name
Object: INVENTORY
Command: DROP TABLE

Min. Ct. 0 | Reset Interval (minutes) 0

Continue to next Rule ☐ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

Merci de votre attention