TENDANCES LOGICIELLES 2008

Mardi 25 mars 2008 – Hilton Arc de Triomphe

ÊTES-VOUS À L'ABRI DE PIRATAGE INFORMATIQUE ?

Test de vulnérabilité des applications Web
avec IBM Rational AppScan

Kamel Moulaoui
Kamel.moulaoui@fr.ibm.com

Sécurité

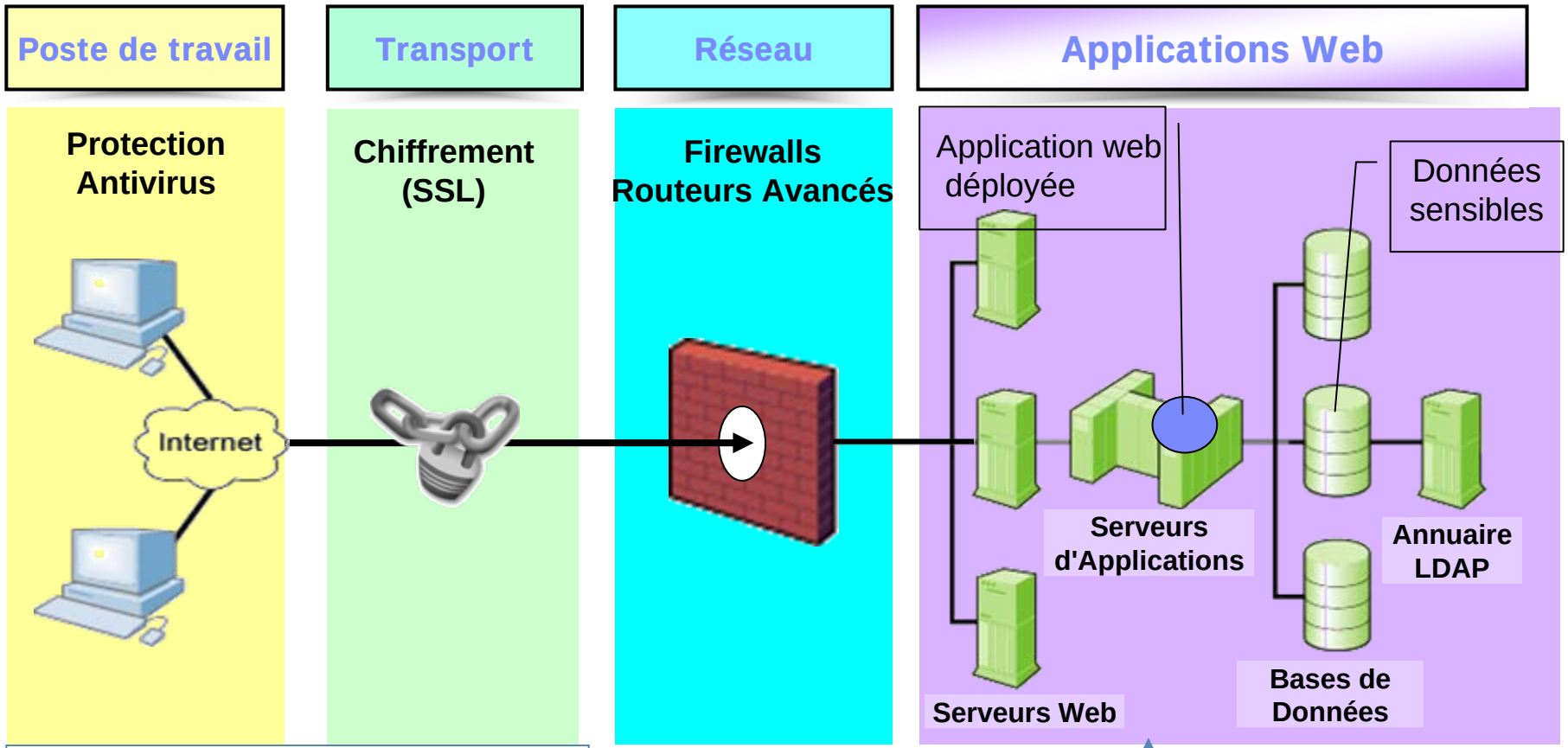
Le mythe : « Notre site est sûr »

Nous avons des Firewalls en place

Nous auditons nos applications périodiquement par des auditeurs externes

Nous utilisons des scanners de vulnérabilité de réseau

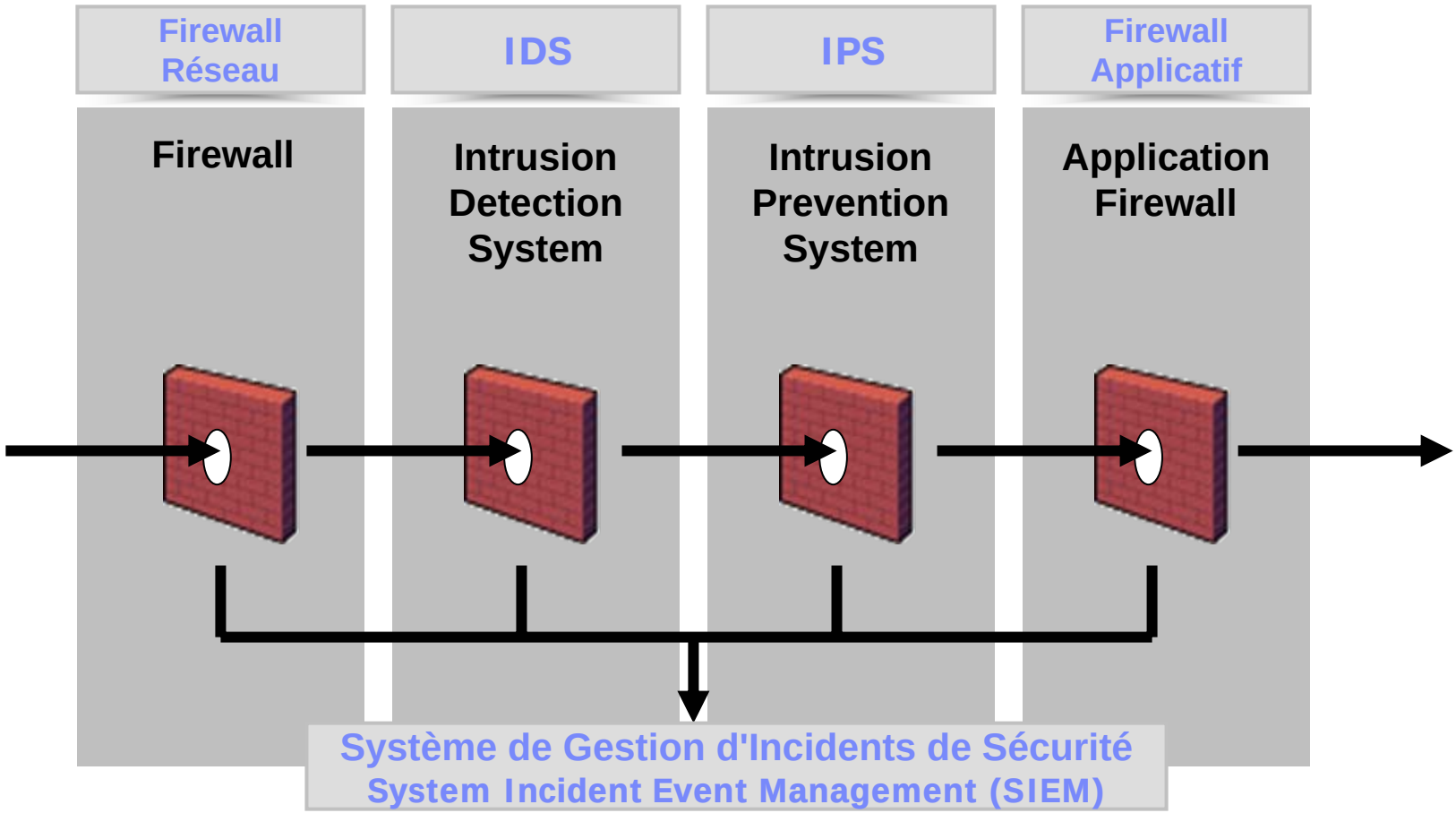
Architecture Globale d'une Application Web Sécurisée



Les solutions de sécurité des applications et des réseaux adressent des problèmes différents

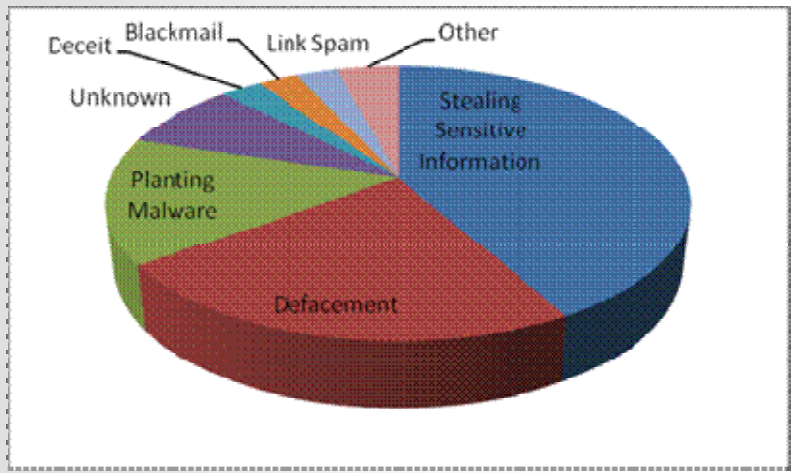
Sécurité

Protections Réseau pour Applications Web



Pourquoi la sécurité applicative est une haute priorité ?

- **Les Applications Web sont la cible #1 des hackers:**
  - 75% des attaques concernent la couche application (Gartner)
  - XSS et SQL Injection sont classées #1 et #2 des vulnérabilités dans le top ten OWASP 2007
- **La plupart des sites sont vulnérables:**
  - 90% des sites sont vulnérables aux attaques d'application (Watchfire)
  - 78% d'applications Web affectées de vulnérabilités facilement exploitables (Symantec)
  - 80% des organisations auront un incident de sécurité d'application d'ici 2010 (Gartner)
- **Les applications Web sont des cibles de valeurs élevées pour les hackers:**
  - Vol d'informations sensibles (données clients, Cartes de crédit, vol et usurpation d'identités) , altération de site, insertion de logiciel malveillants, etc.
- **Exigences de conformité:**
  - Payment Card Industry (PCI) Standards, Sarbanes Oxley, ISO.



Statistiques des vulnérabilités pour 2007 selon WASC

Attack/Vulnerability Used	%
SQL Injection	20%
Unintentional Information Disclosure	17%
Known Vulnerability	15%
Cross Site Scripting (XSS)	12%
Insufficient Access Control	10%
Credential/Session Prediction	8%
OS Commanding	3%
Misconfiguration	3%
Insufficient Anti-automation	3%
Denial of Service	3%
Redirection	2%
Insufficient Session Expiration	2%
Cross Site Request Forgery (CSRF)	2%

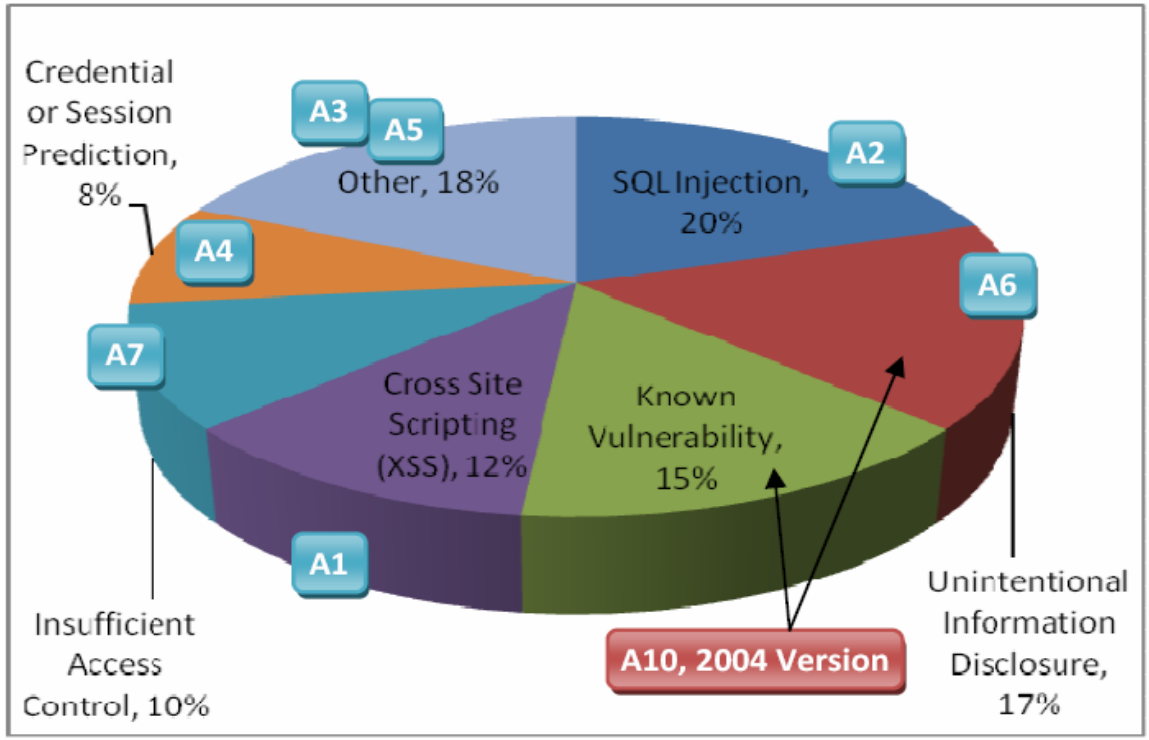
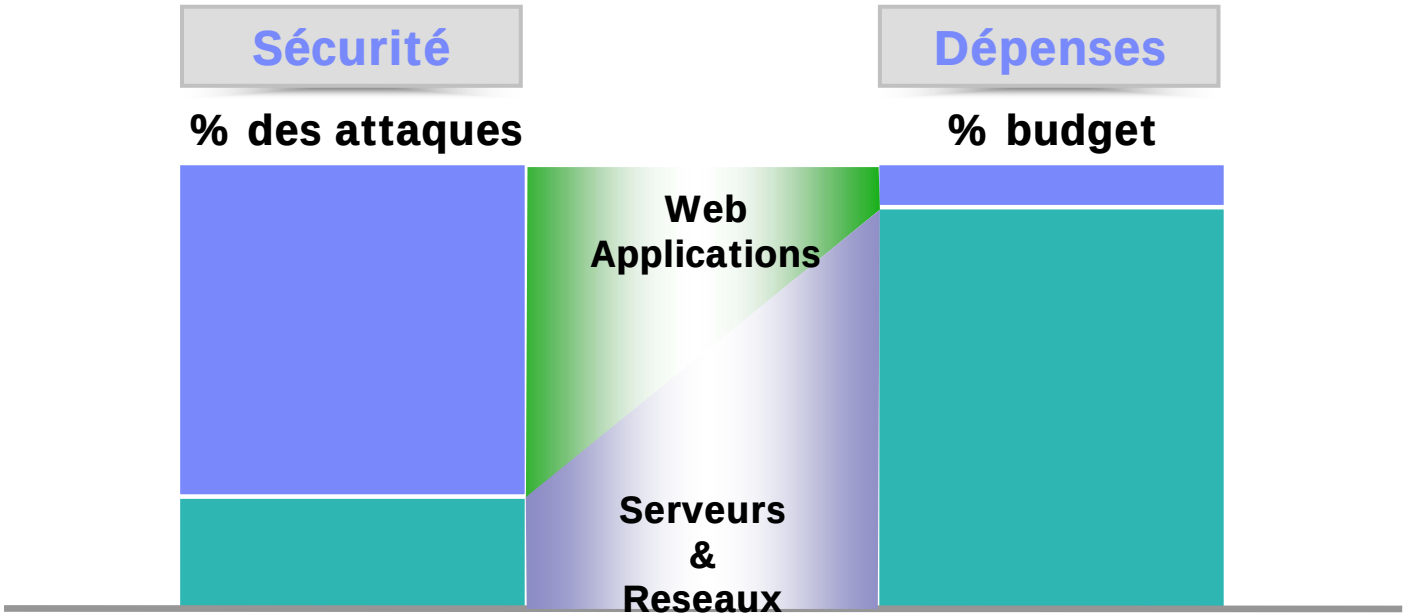


FIGURE 3 -INCIDENT BY ATTACK METHOD
("A" LABELS REFER TO THE OWASP TOP 10 POSITION)

La sécurité et les dépenses ne sont pas équilibrées



75% Des attaques sur la sécurité de l'information sont dirigées vers la couche application web

2/3 De toutes les applications Web son vulnérables

Gartner

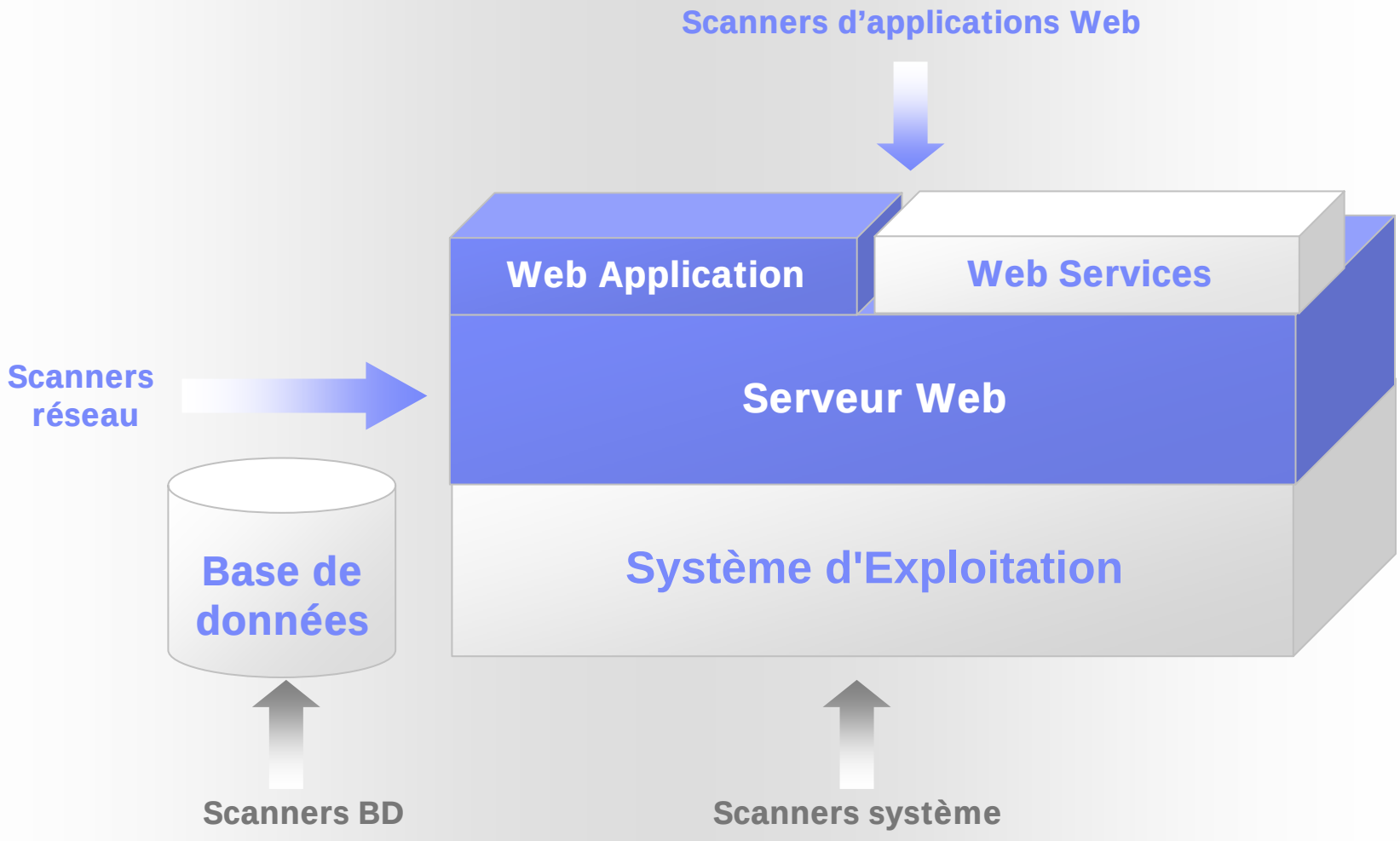
Sources: Gartner, Watchfire

Vulnérabilités "Héritées" vs Vulnérabilités "Générées"

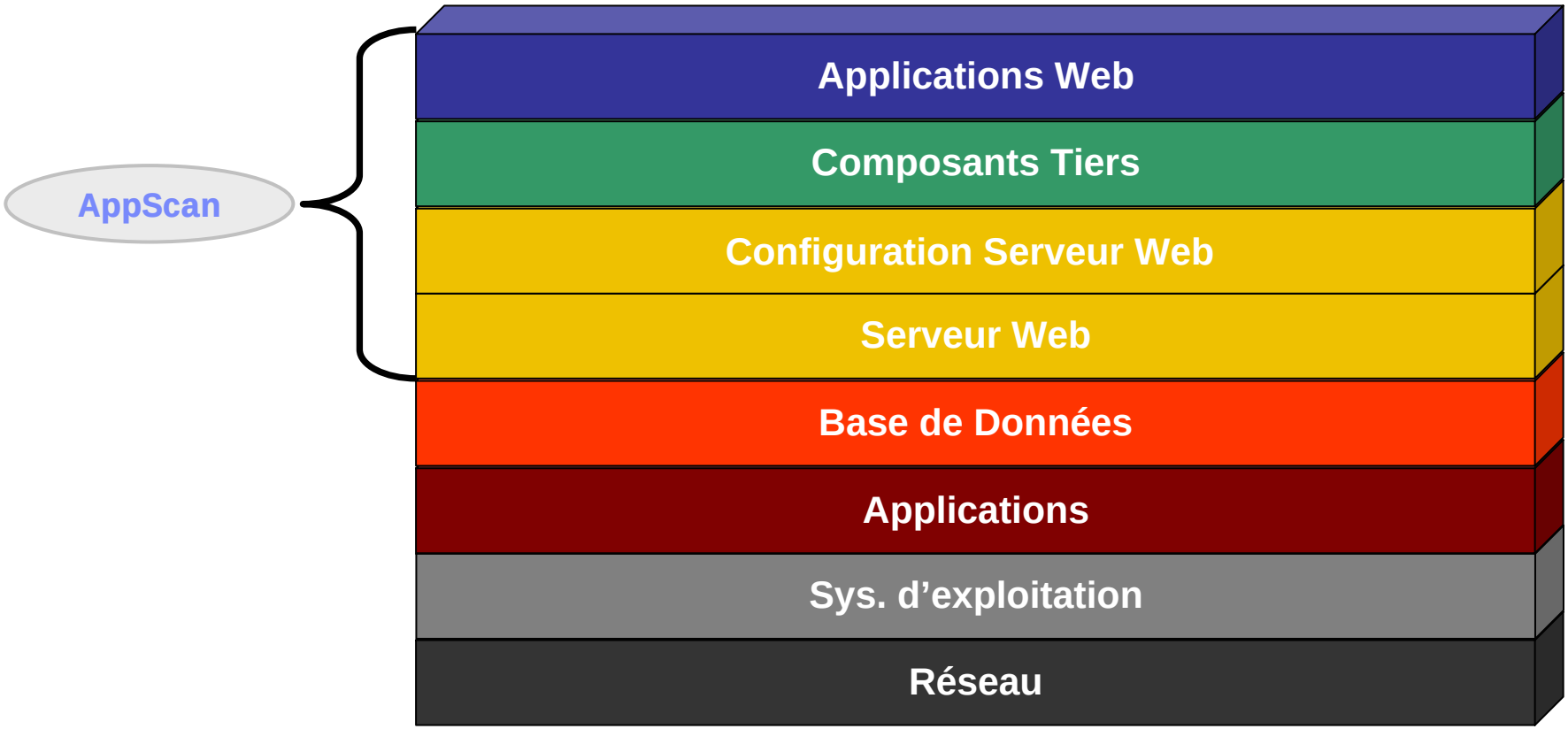
	CWV Common Web Vulnerabilities	ASV Application Specific Vulnerabilities
Localisation	**Composants** d'infrastructure et autres **progiciels tiers**	**Applications métier** spécifiques à l'entreprise
Origine	Code non sécurisé développé par les **éditeurs de logiciels**	Code non sécurisé développé par les **équipes internes** (ou les sous-traitants**)**
Information Disponible	Descriptions publiées par les éditeurs et répertoriées par différents organismes (référence CVE)	Aucune
Détection	Vérification de signatures et contrôle des configurations	Tests spécifiques à chaque page, chaque paramètre, chaque cookie etc.
Actions Correctives	Appliquer les patches fournis par les éditeurs	Instaurer un processus de contrôle sécurité sur tout le cycle de vie du logiciel
Coût de la Sécurisation	**Relativement faible**: coût de la gestion de patches.	**Très élevé**, si le processus reste manuel et réactif.

Sécurité

Environnement d'une application Web



Quels sont les composants testés par AppScan ?

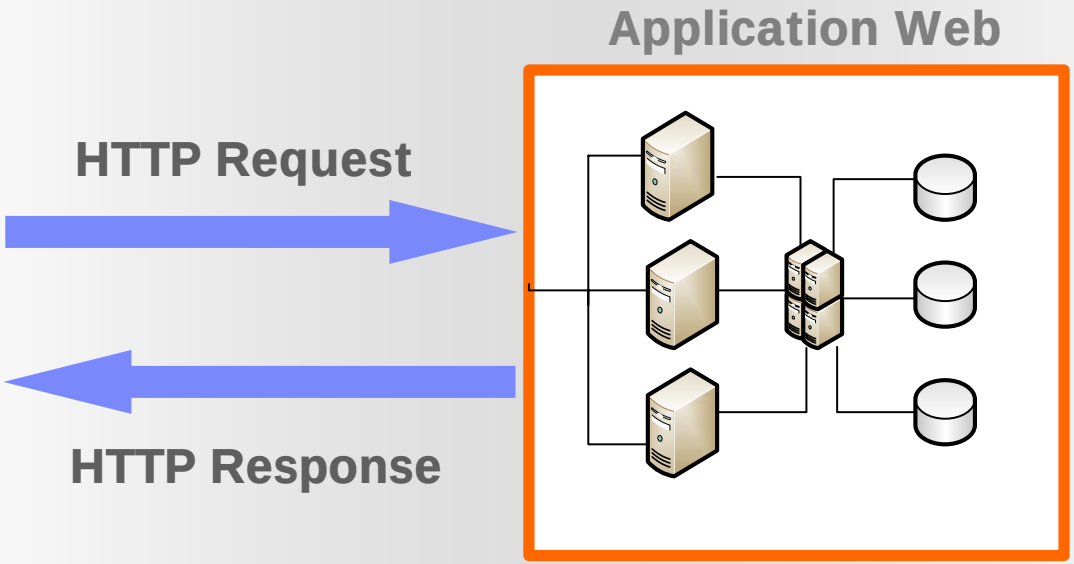


Rational AppScan

- Qu'est ce qu'AppScan ?
  - AppScan est un outil de test automatisé, utilisé pour réaliser des évaluations et des audits de vulnérabilité sur des applications et des services Web
- Pourquoi?
  - Pour simplifier la recherche et la correction des problèmes de sécurité des applications Web .
- Que fait AppScan?
  - Scan les applications Web, recense les failles et problèmes de sécurité trouvés sur l'application, génère un rapport incluant des conseils et de recommandations sur les corrections à réaliser.
- Qui l'utilise?
  - Auditeurs de sécurité - utilisateurs principaux aujourd'hui
  - Ingénieurs AQ - quand les auditeurs deviennent le goulot d'étranglement
  - Développeurs – Pour détecter très tôt les problèmes de sécurité dans applications en phase de developpement (plus efficace)

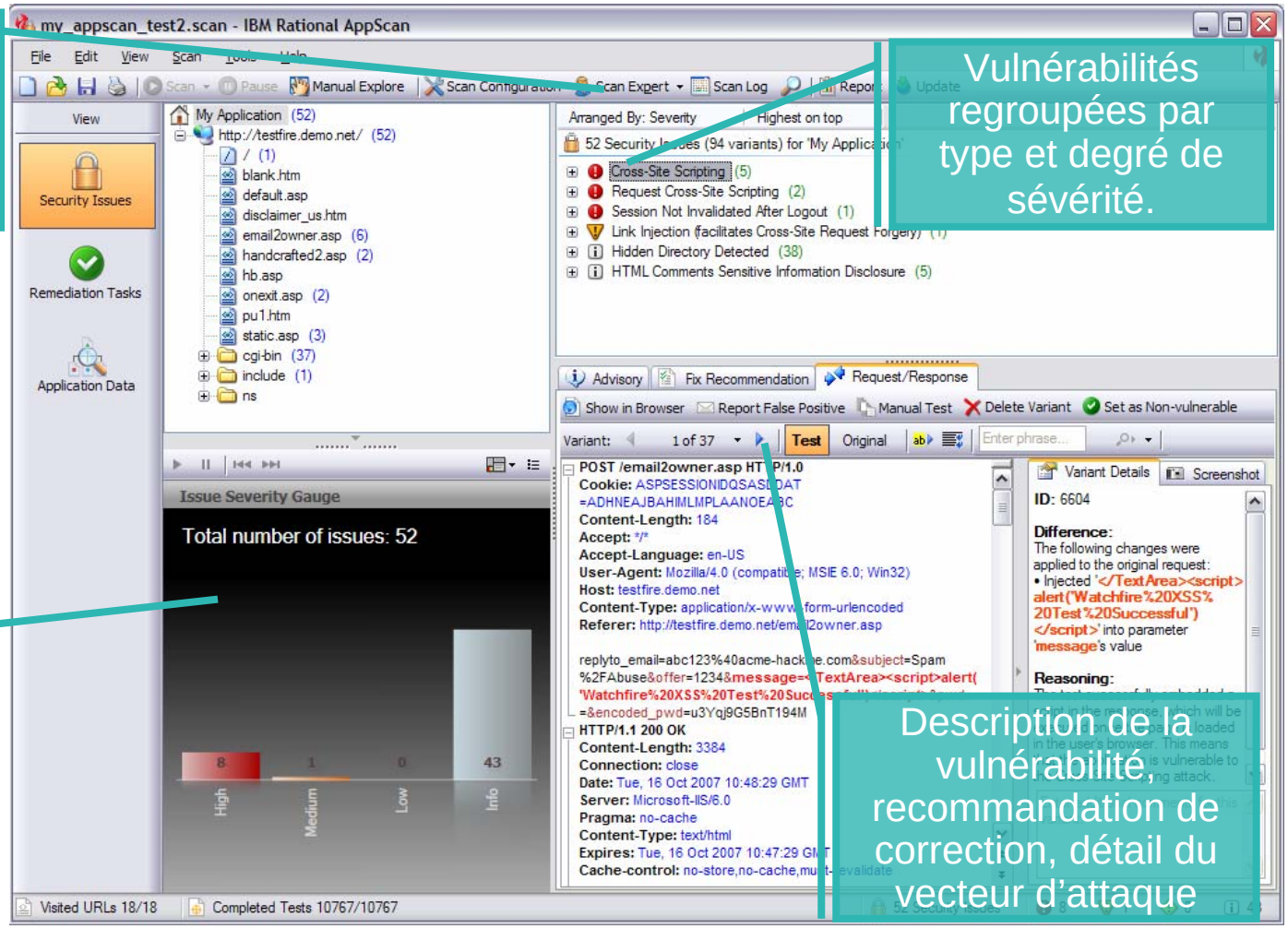
AppScan: Principe de fonctionnement

- Aborde l'application comme une boite noire
- Parcourt l'application web et construit un modèle du site
- Détermine les vecteurs d'attaque basés sur la politique choisie du test
- Teste en envoyant des requêtes HTTP modifiées à l'application et en examinant les réponses HTTP selon les règles de validations.
- Génère un rapport incluant des conseils et de recommandations sur les corrections à réaliser.



Rational AppScan

Générateur de rapports puissant



Vulnérabilités regroupées par type et degré de sévérité.

Suivi du nombre de vulnérabilités pendant le test

Description de la vulnérabilité, recommandation de correction, détail du vecteur d'attaque

Modèle de maturité de la sécurité applicative

Stratégique

- Contrôle sécurité sur tout le cycle de vie des applications
- Métriques au niveau entreprise pour l'ensemble des applications

Tactique

- Experts internes, audits réguliers
- Outils d'audit de type "desktop"

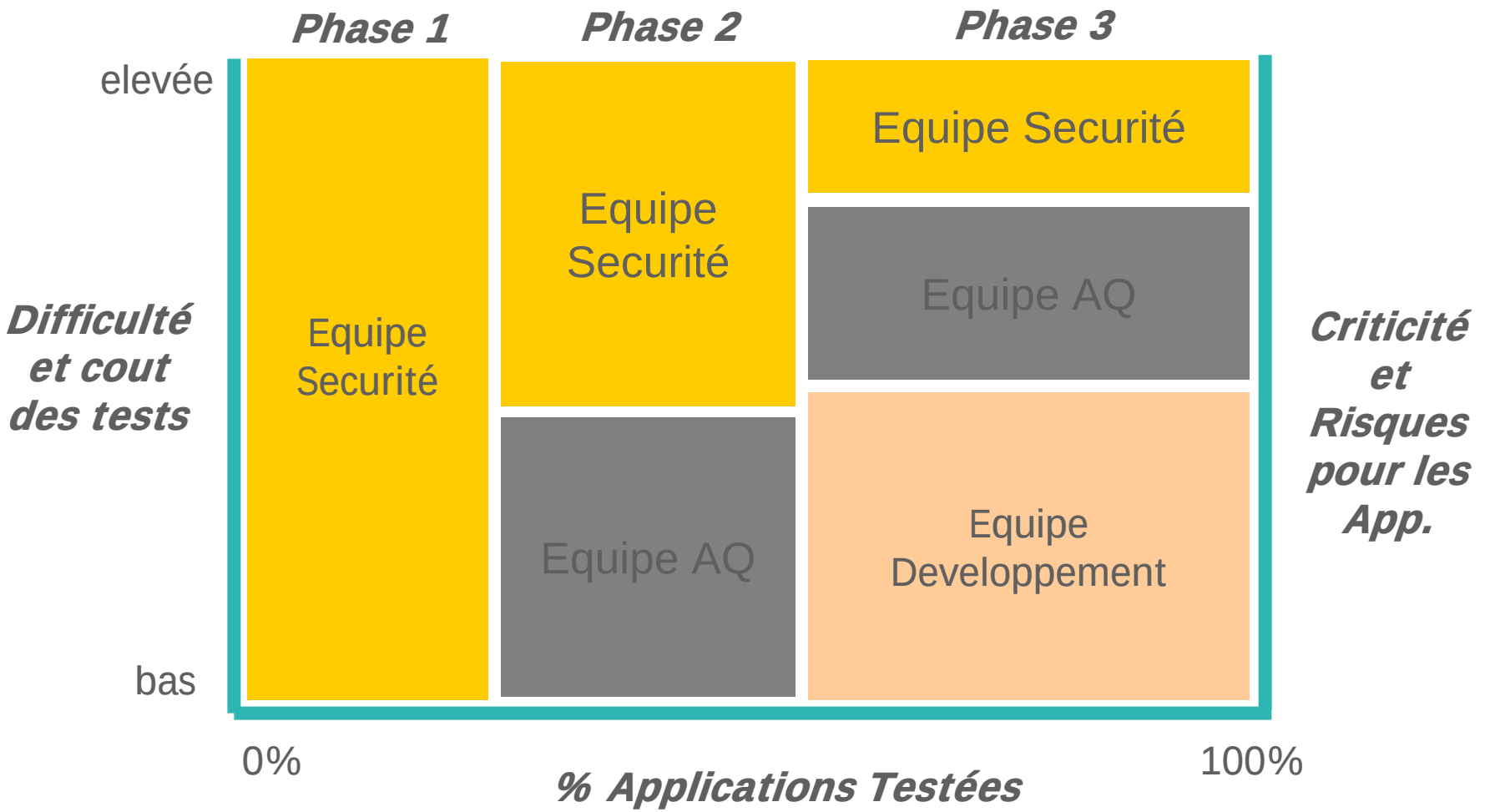
Audits internes

- Équipe interne dédiée aux tests et audits de sécurité des applications

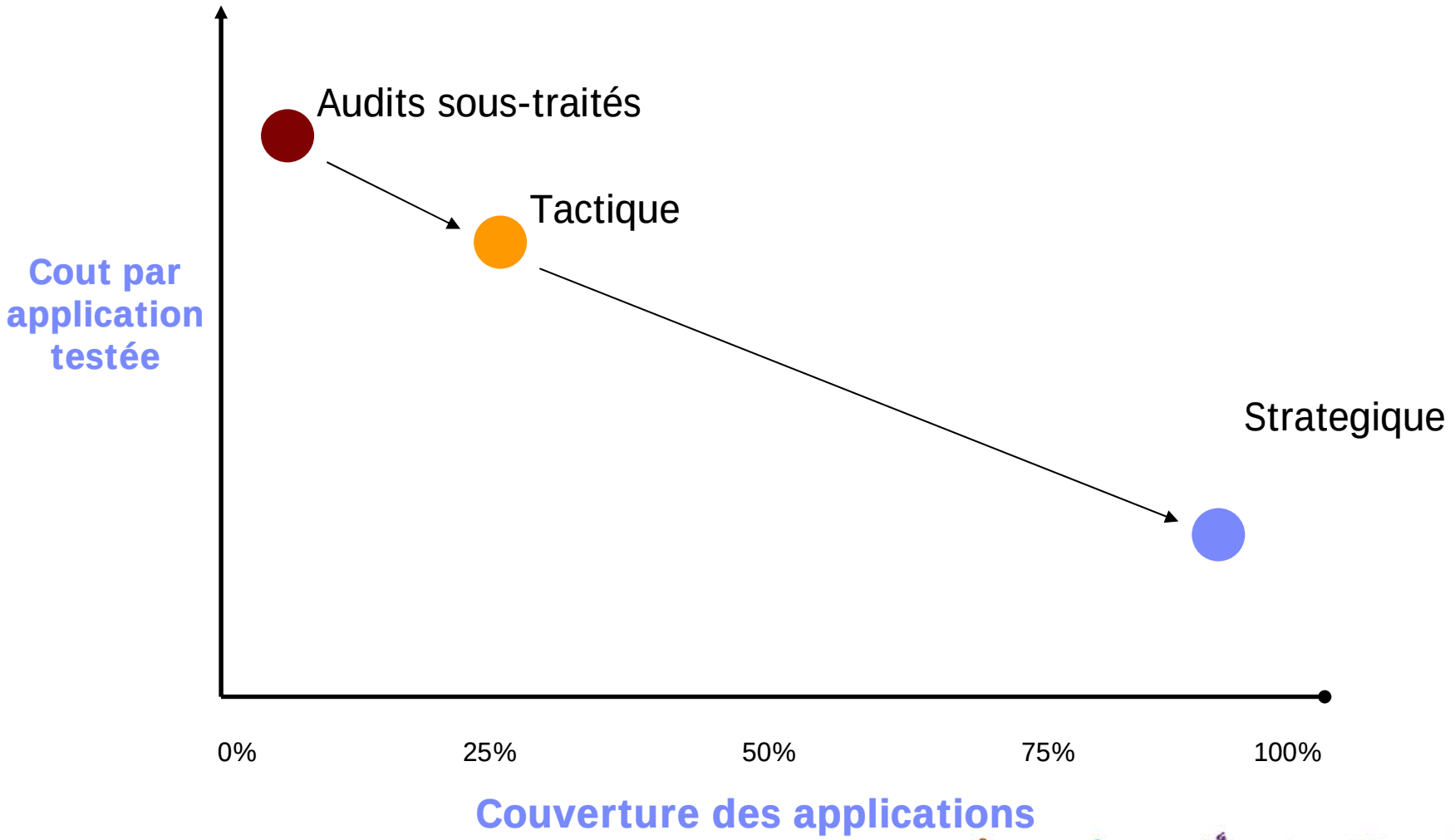
Audits sous-traités

- Consultants, tests de pénétration sur quelques applications critiques

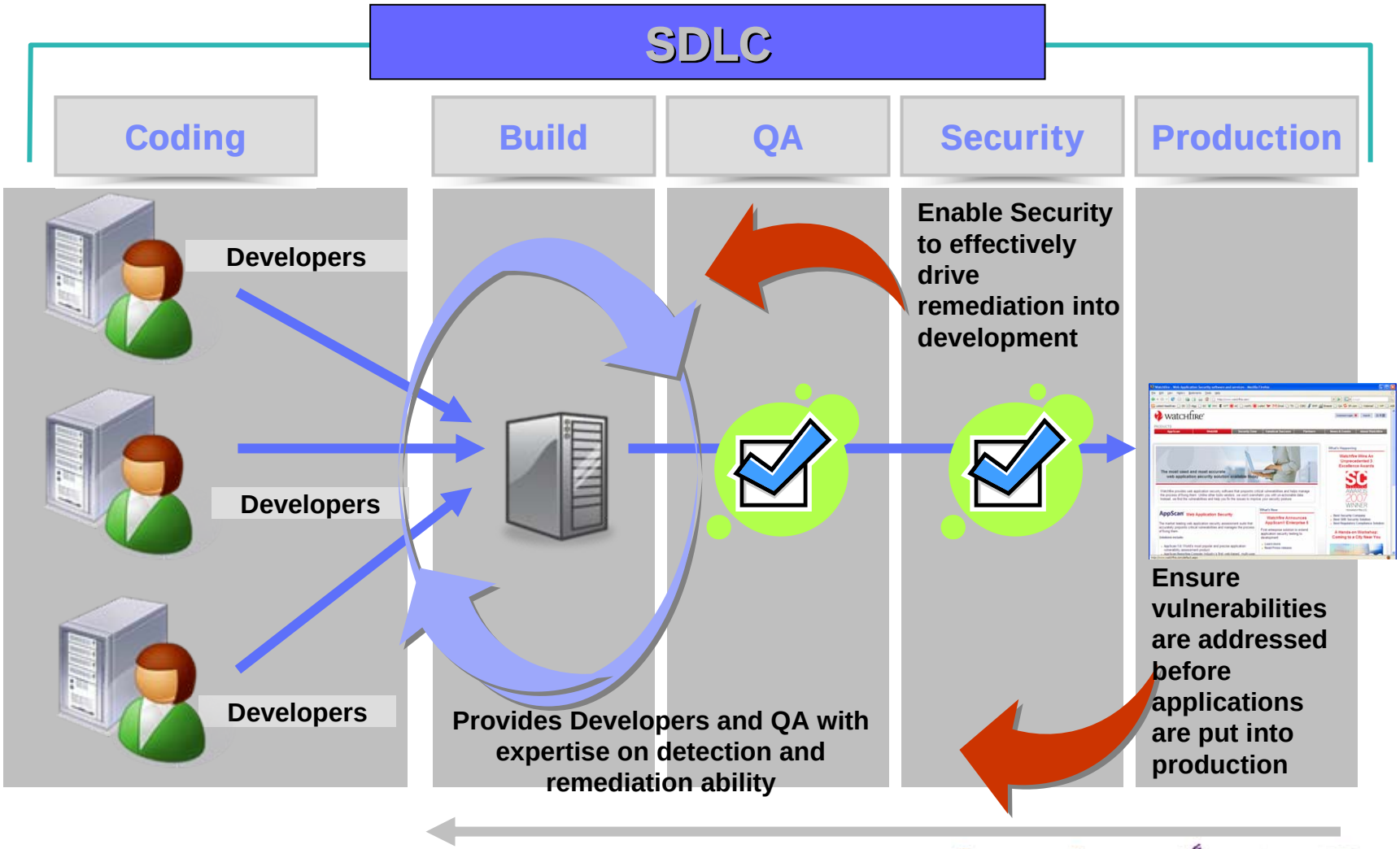
Modèle de maturité de la sécurité applicative



Reduire les couts, Etendre la couverture

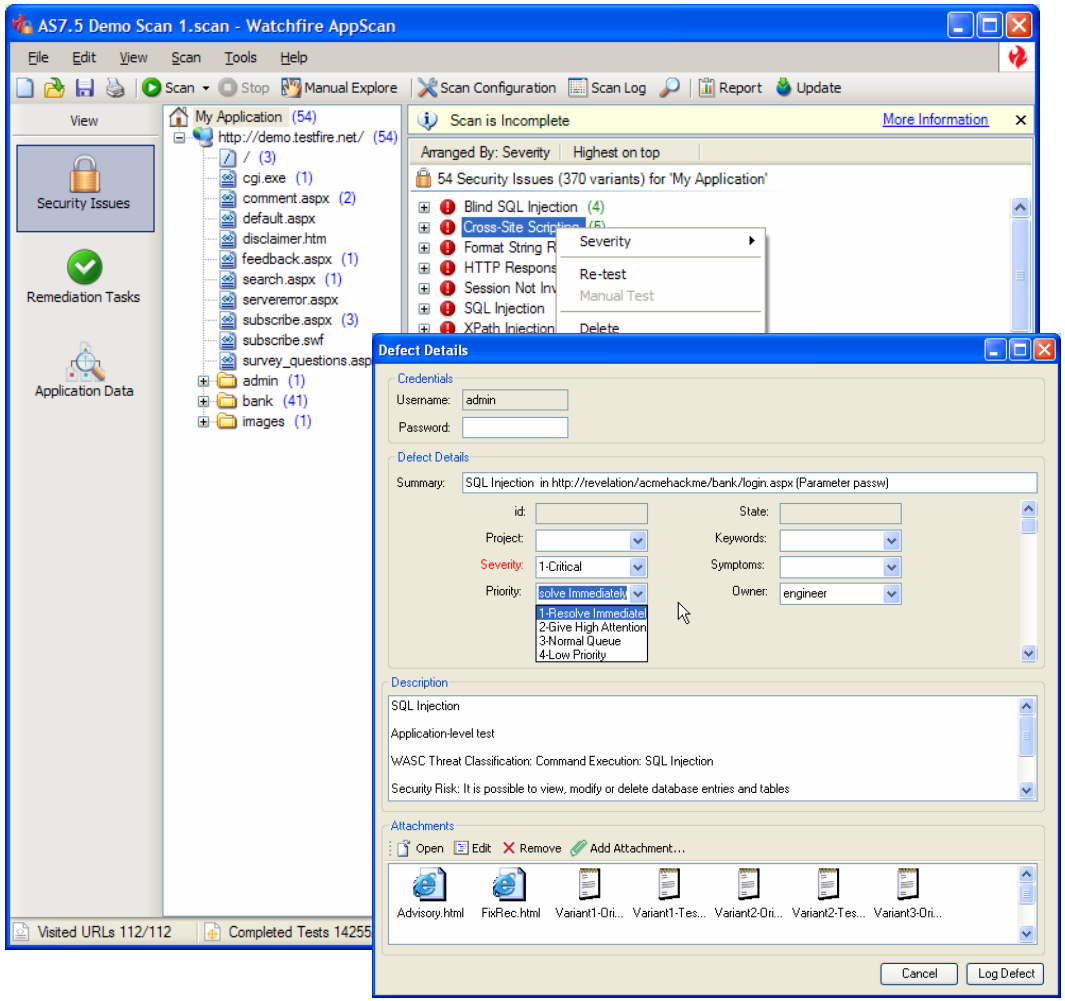


Sécurité et conformité dans le processus de devp.



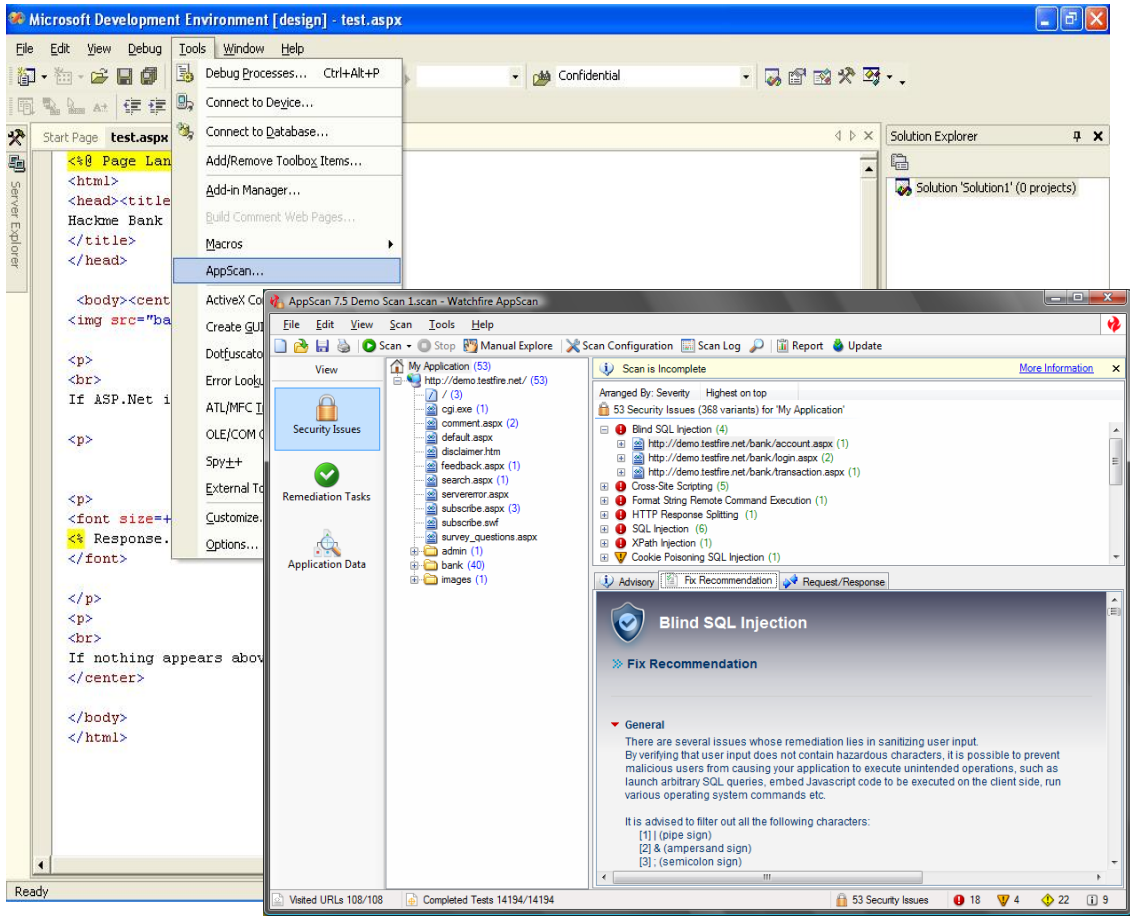
Intégrer la sécurité dans le processus d'Assurance Qualité

- Suivre la correction des vulnérabilités au même titre que les autres "bugs"
- Rational AppScan injecte les vulnérabilités trouvées, dans des outils de "bug tracking", tels que:
  - IBM Rational ClearQuest

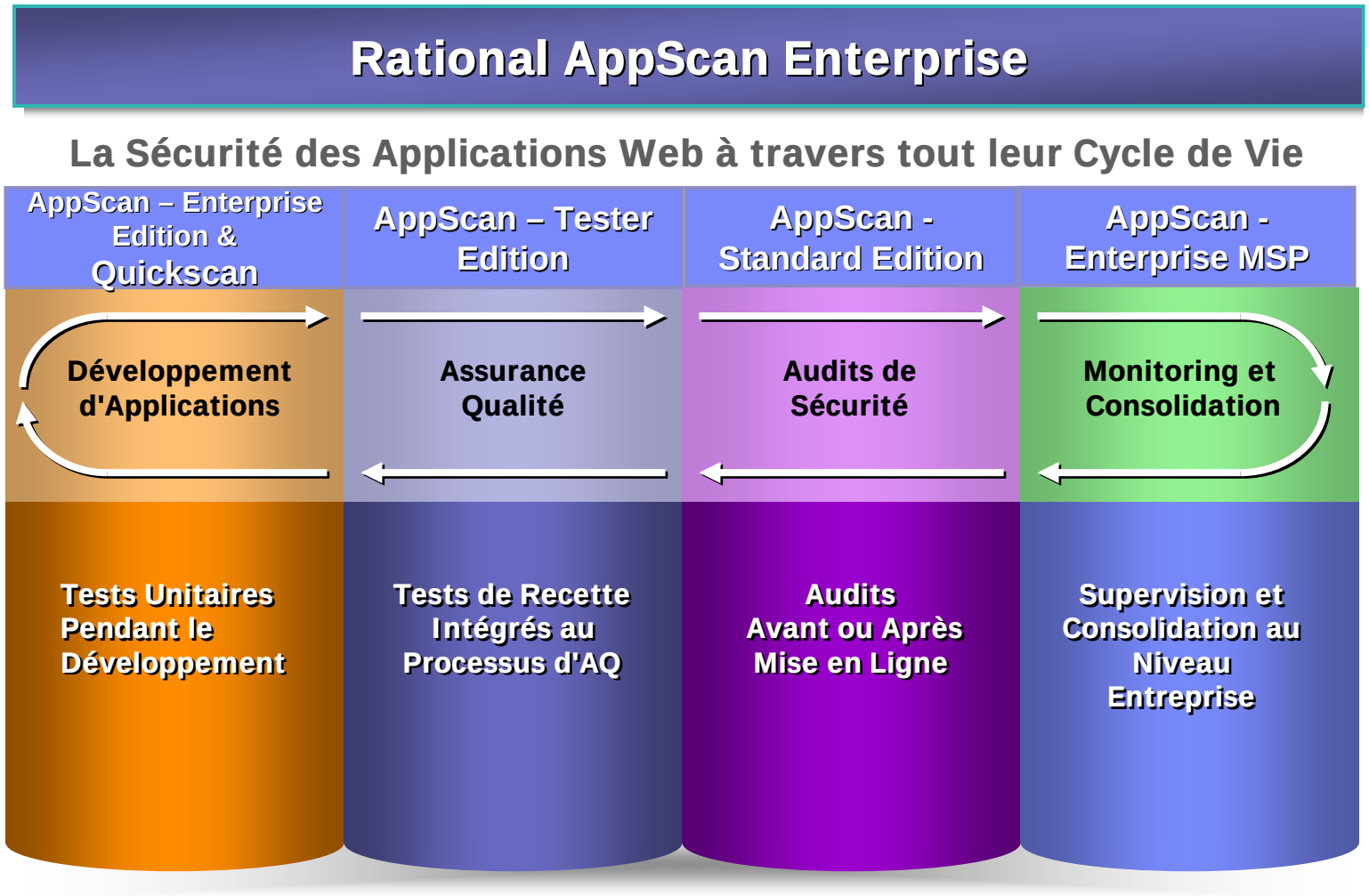


Détecter et corriger au plus tôt les vulnérabilités applicatives

- AppScan permet au développeur de tester ses transactions et services dés leur mise au point, depuis son environnement de travail
- Il peut être intégré dans **Eclipse**, **Websphere**, **JBuilder** ou **Visual Studio.Net**
- AppScan effectue les tests applicatifs et offre des explications et aides à la correction spécifiques à l'environnement



Famille des produits Rational AppScan



AppScan Enterprise

Solution Évolutive, basée sur le client Web, pour gérer la sécurité des applications Web.

+ de 800 Entreprises font Confiance à Watchfire

9 des 10 1ères Banques	8 des 10 1ères Sociétés High-Tech	7 des 10 1ers Groupes Pharmaceutiques	Plusieurs Grandes Administrations
HSBC	Microsoft	Wyeth	
JPMorganChase	Cisco Systems	Novartis	
citi	intel	AstraZeneca	
AXA Financial Protection	DELL	Abbott Laboratories	
Fidelity	IBM	Aventis	
SunTrust	SONY		
Liberty Mutual	Adobe	Roche	
Sovereign Bank	Analog Devices	Genentech	United States Postal Service

FRANCE:

- Accor
- Business Objects
- EDF
- France Telecom
- Gaz de France
- Total
- Vente-Privée

- Sur www.watchfire.com vous trouverez une liste plus complète, par secteur d'activité et certaines "success stories"

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 <u>gratuitement</u> :

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

- 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 …

Pour en savoir plus:

- IBM Rational software
- IBM Rational Software Delivery Platform
- Process and portfolio management
- Change and release management
- Quality management
- Architecture management
- Rational trial downloads
- developerWorks Rational
- IBM Rational TV
- IBM Rational Business Partners