

*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 »

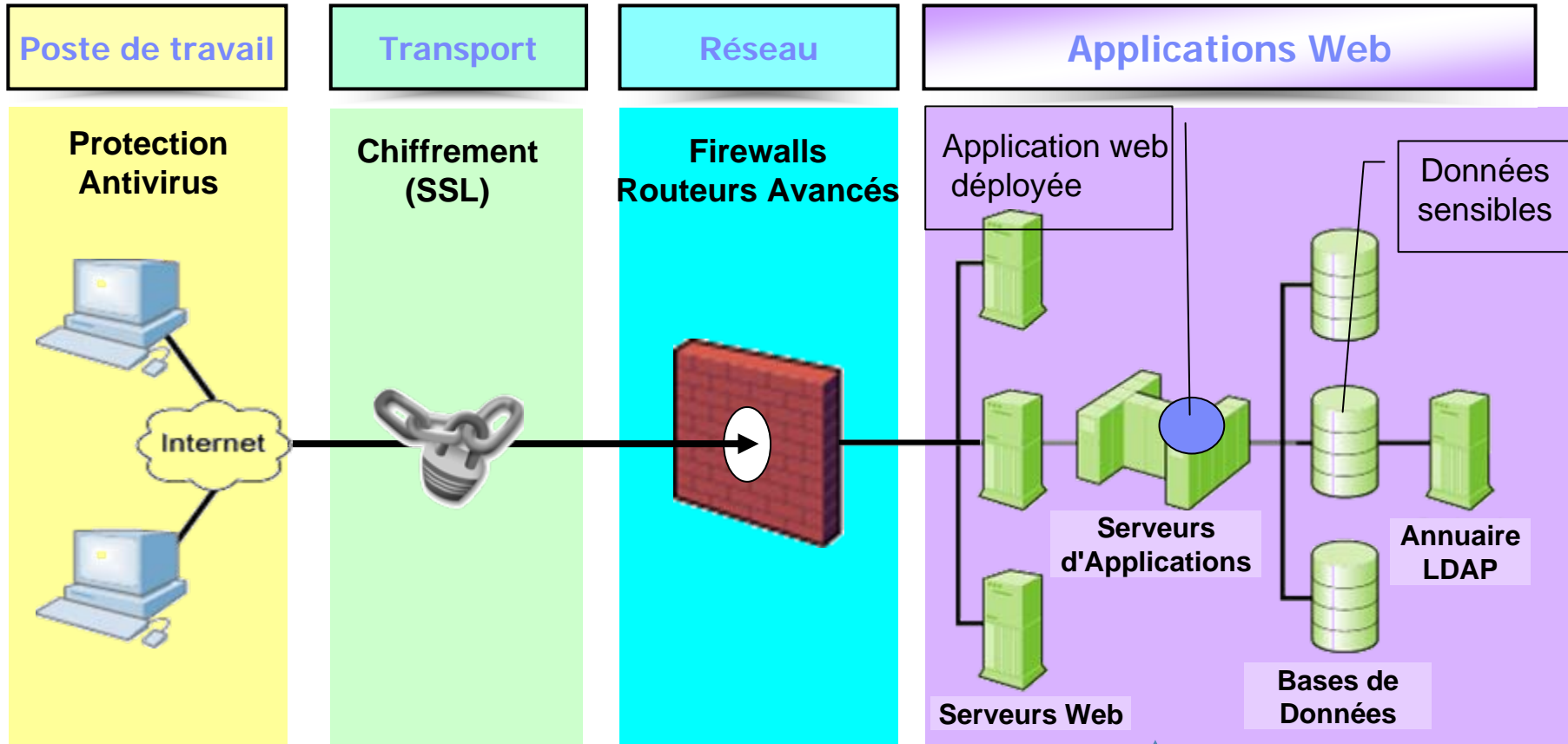
Nous avons des  
Firewalls en place

Nous auditons nos  
applications  
périodiquement par des  
auditeurs externes

Nous utilisons des  
scanners de vulnérabilité  
de réseau



# Architecture Globale d'une Application Web Sécurisée

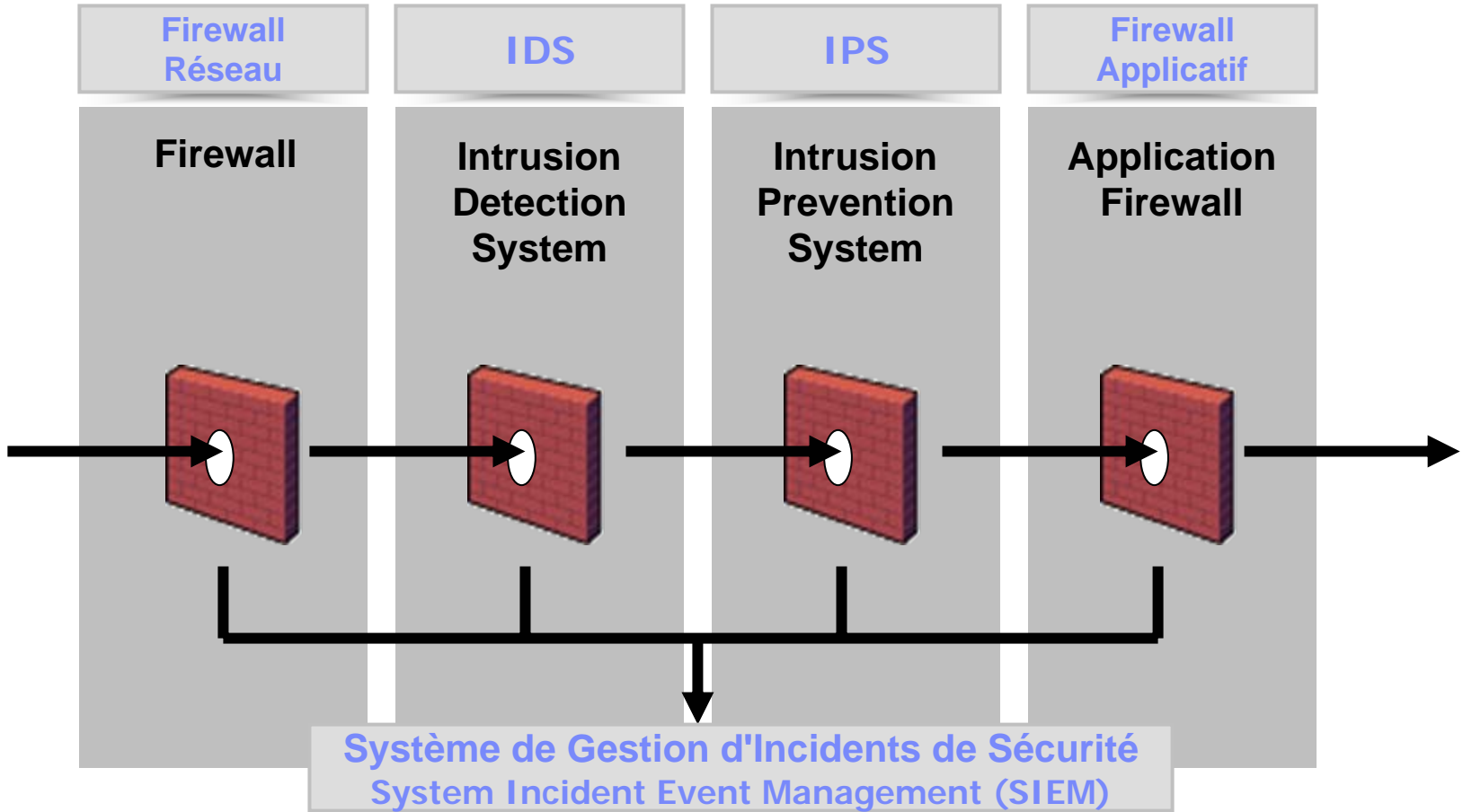


Les solutions de sécurité des applications et des réseaux adressent des problèmes différents



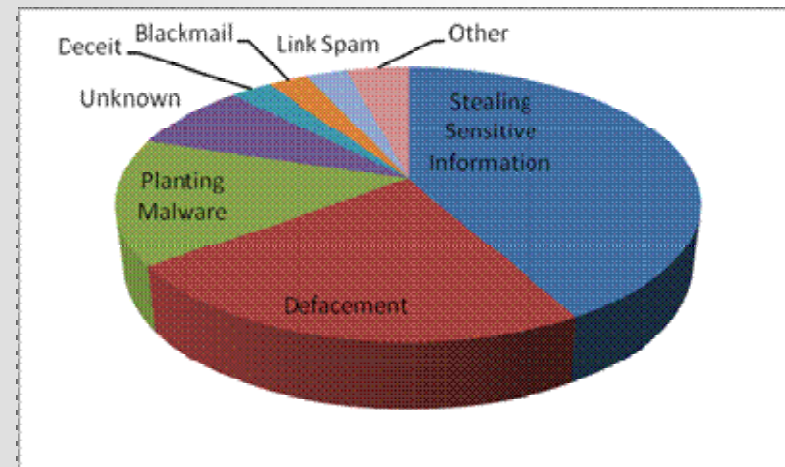


# Protections Réseau pour Applications Web



# 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%

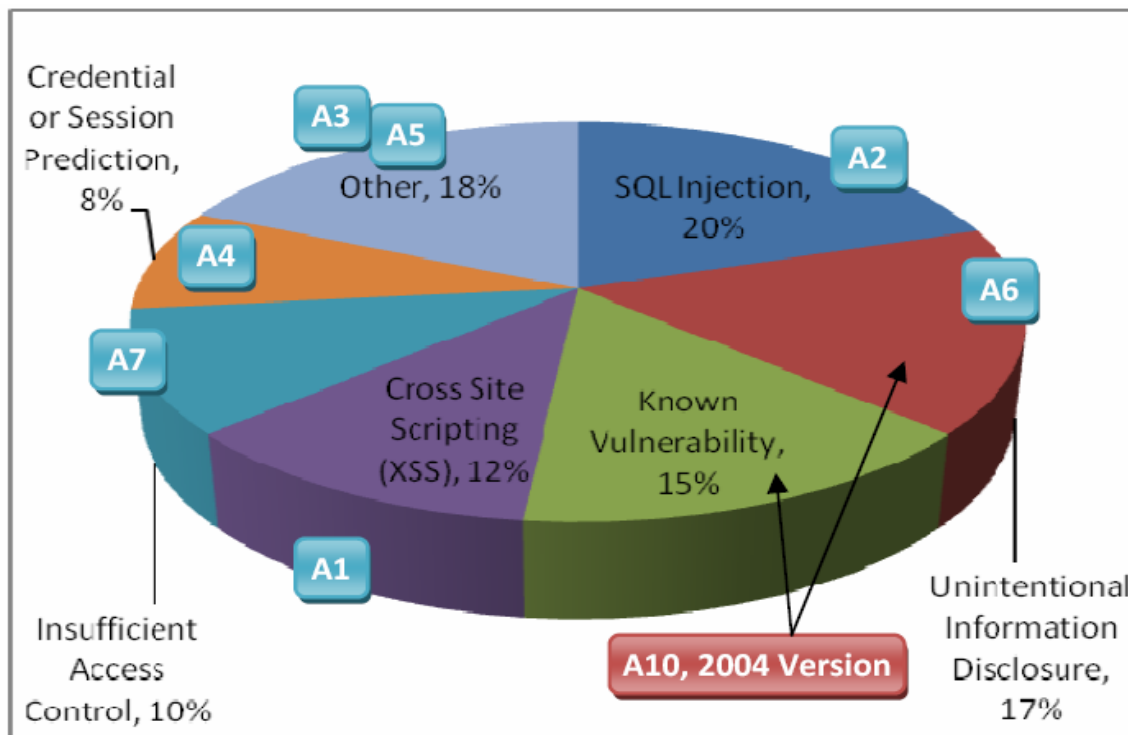


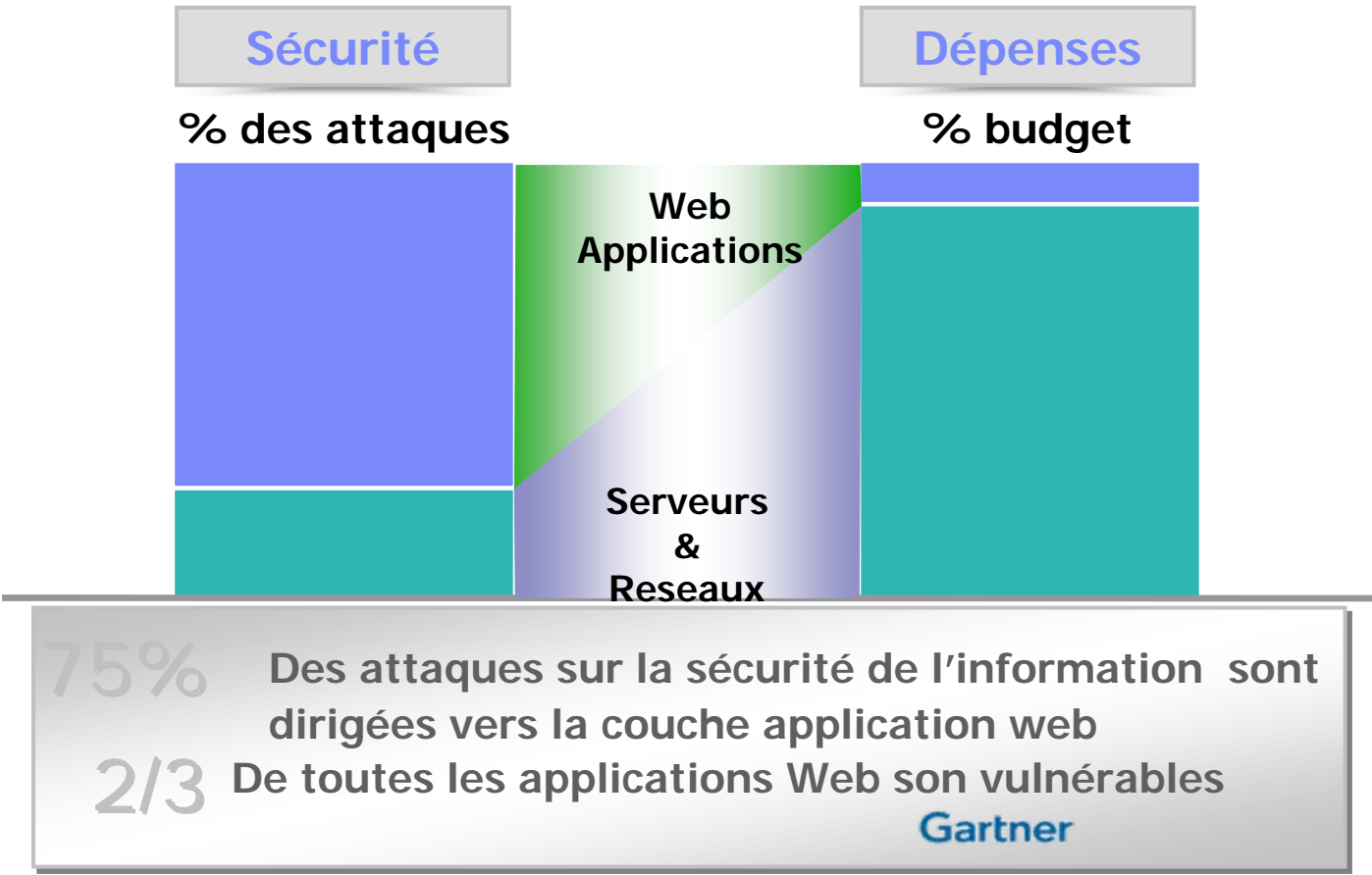
FIGURE 3 - INCIDENT BY ATTACK METHOD  
("A" LABELS REFER TO THE OWASP TOP 10 POSITION)







# La sécurité et les dépenses ne sont pas équilibrées



Sources: Gartner, Watchfire





# Vulnérabilités "Héritées" vs Vulnérabilités "Générées"

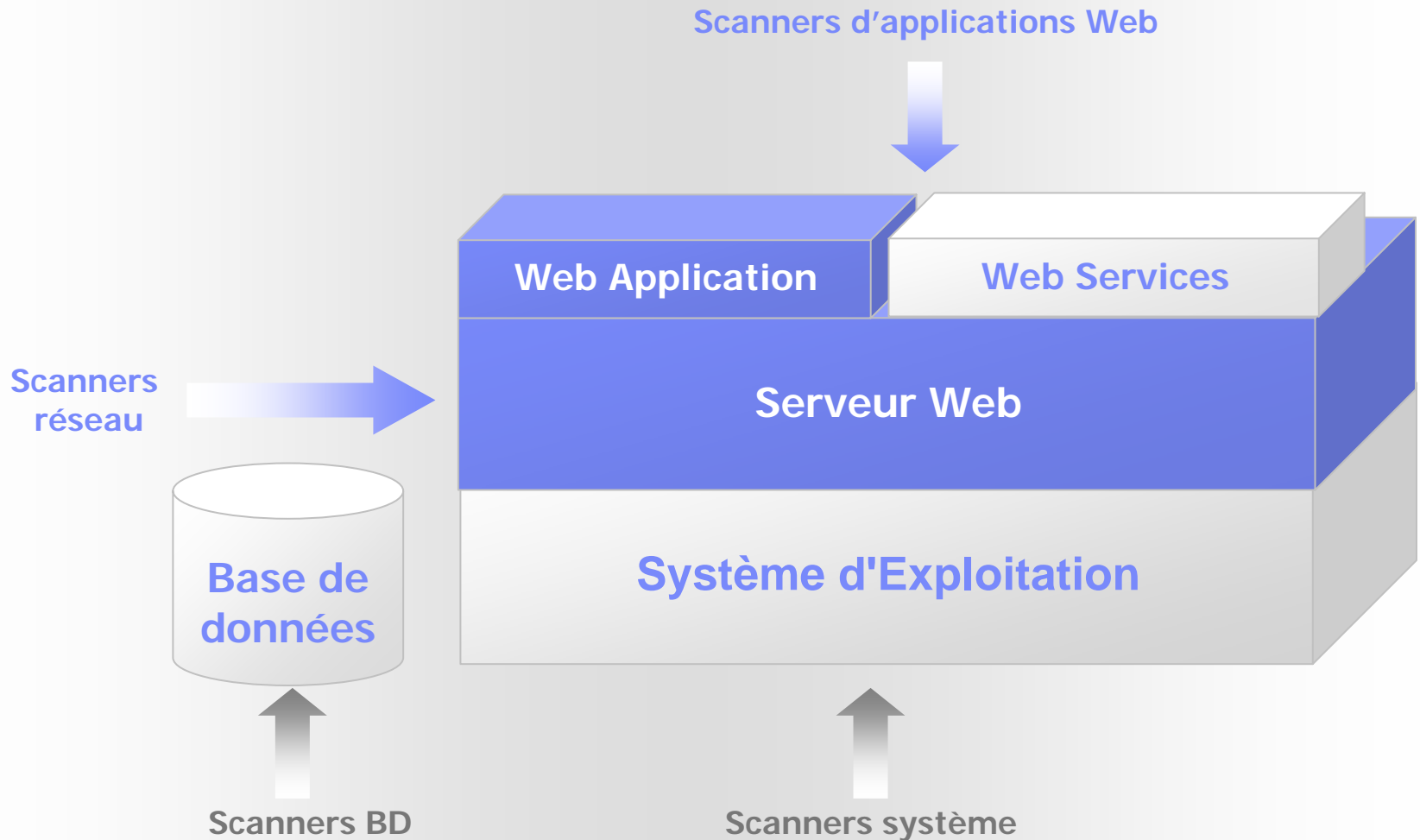
	CWV Common Web Vulnerabilities	ASV Application Specific Vulnerabilities
Localisation	<b>Composants</b> d'infrastructure et autres <b>progiciels tiers</b>	<b>Applications métier</b> spécifiques à l'entreprise
Origine	Code non sécurisé développé par les <b>éditeurs de logiciels</b>	Code non sécurisé développé par les <b>équipes internes</b> (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	<b>Relativement faible</b> : coût de la gestion de patches.	<b>Très élevé</b> , si le processus reste manuel et réactif.



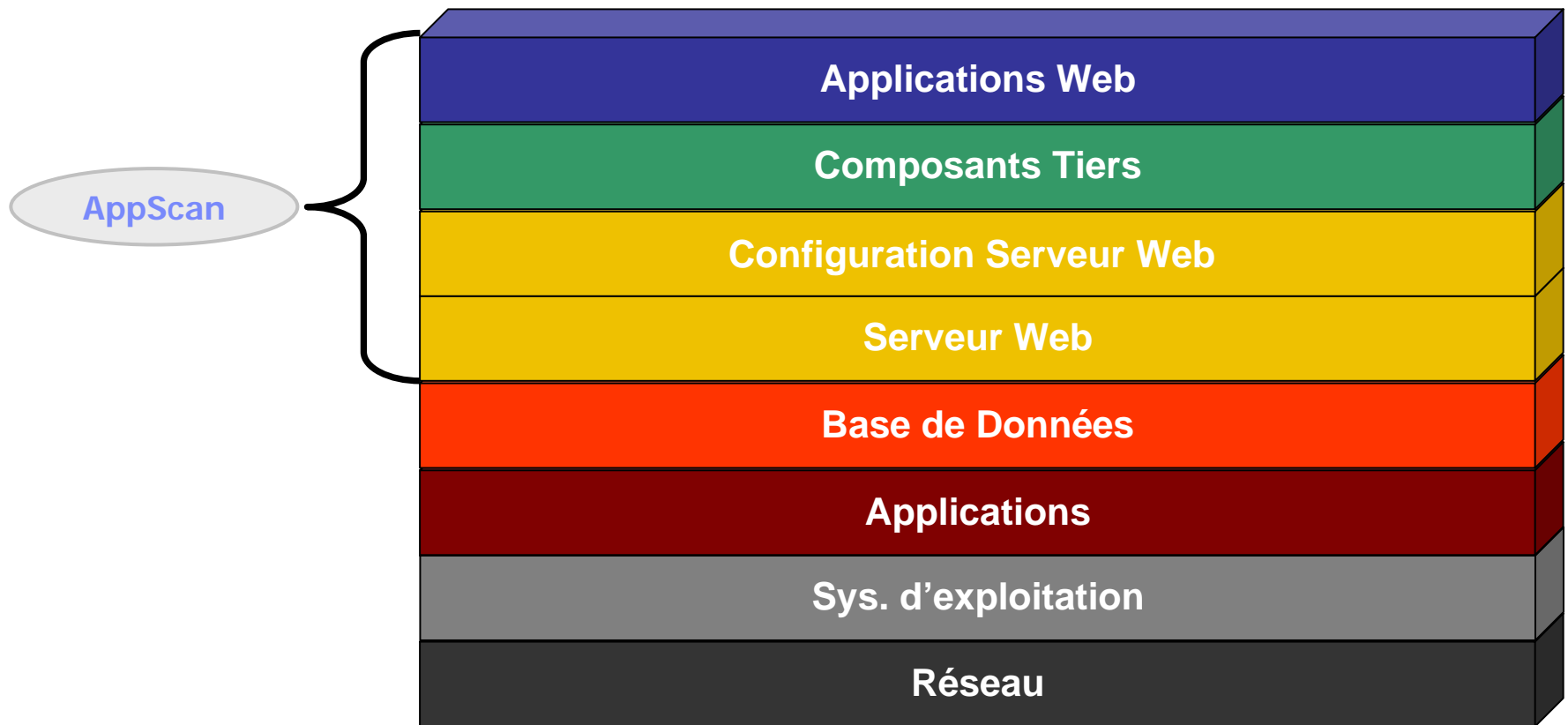


Sécurité

# Environnement d'une application Web



# Quels sont les composants testés par AppScan ?

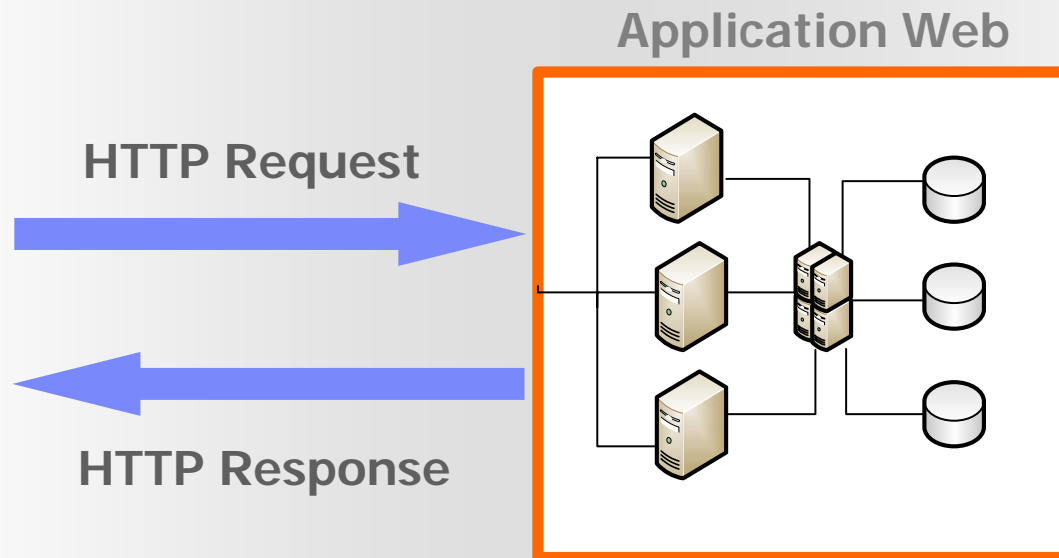


# Rational AppScan

- 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 boîte 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.

Issue Severity Gauge

Total number of issues: 52

High	Medium	Low	Info
8	1	0	43

Variant: 1 of 37

Test Original

```

POST /email2owner.asp HTTP/1.0
Cookie: ASPSESSIONIDQSAJDAT=ADHNEAJBAHMLMPLAANOEA3C
Content-Length: 184
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: testfire.demo.net
Content-Type: application/x-www-form-urlencoded
Referer: http://testfire.demo.net/email2owner.asp

replyto_email=abc123%40acme-hackme.com&subject=Spam
%2FAbuse3offer=1234&message=<script>alert('Watchfire%20XSS%20Test%20Successful')</script>
=3encoded_pwd=u3Yqj9G5BnT194M
HTTP/1.1 200 OK
Content-Length: 3384
Connection: close
Date: Tue, 16 Oct 2007 10:48:29 GMT
Server: Microsoft-IIS/6.0
Pragma: no-cache
Content-Type: text/html
Expires: Tue, 16 Oct 2007 10:47:29 GMT
Cache-control: no-store,no-cache,must-revalidate
    
```

Variant Details

ID: 6604

Difference:

The following changes were applied to the original request:

- Injected '</TextArea><script>alert('Watchfire%20XSS%20Test%20Successful')</script>' into parameter 'message's value

Reasoning:

The injected payload is loaded in the user's browser. This means the user is vulnerable to a script attack.

Suivi du nombre de vulnérabilités pendant le test

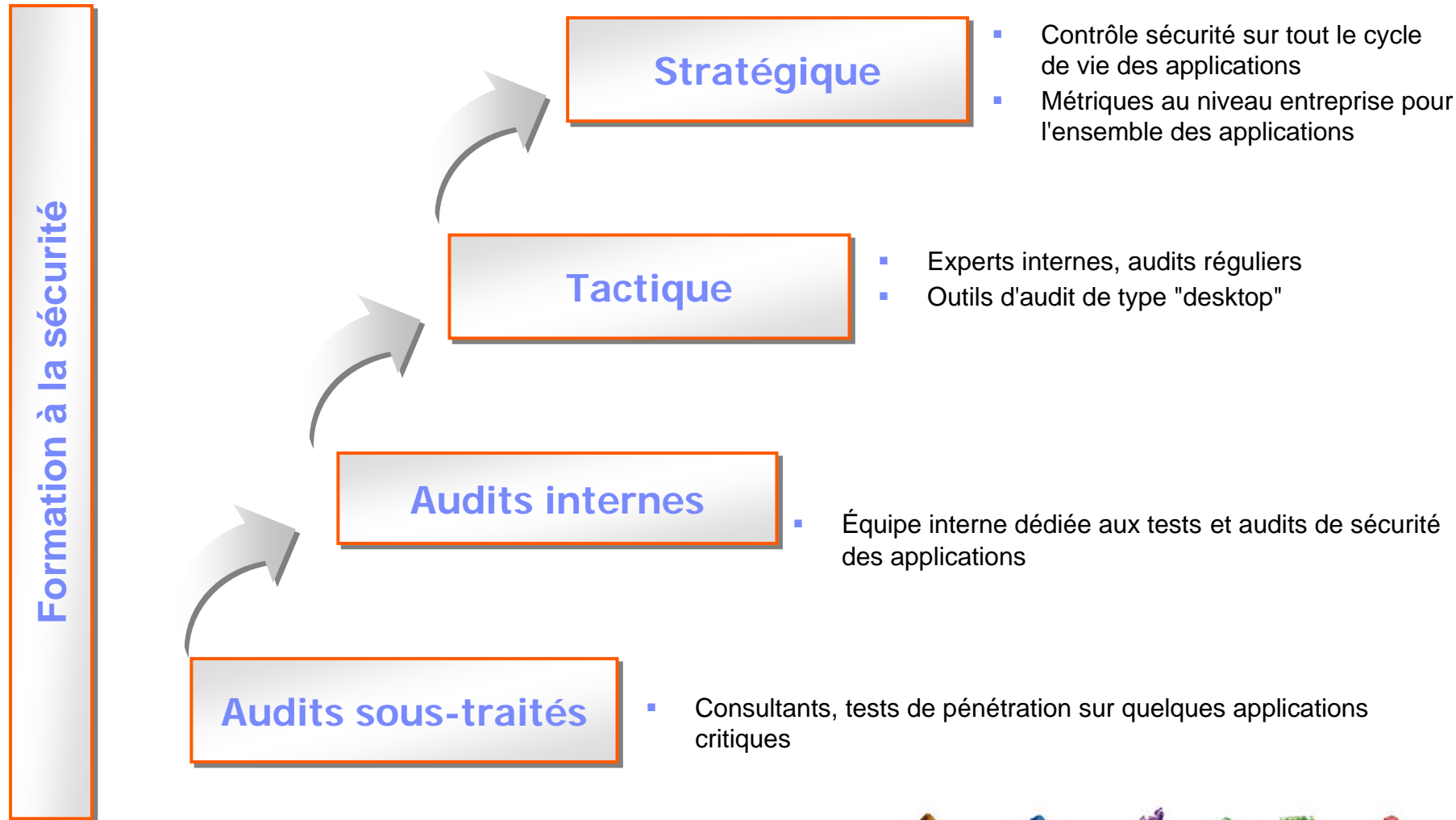
Description de la vulnérabilité, recommandation de correction, détail du vecteur d'attaque



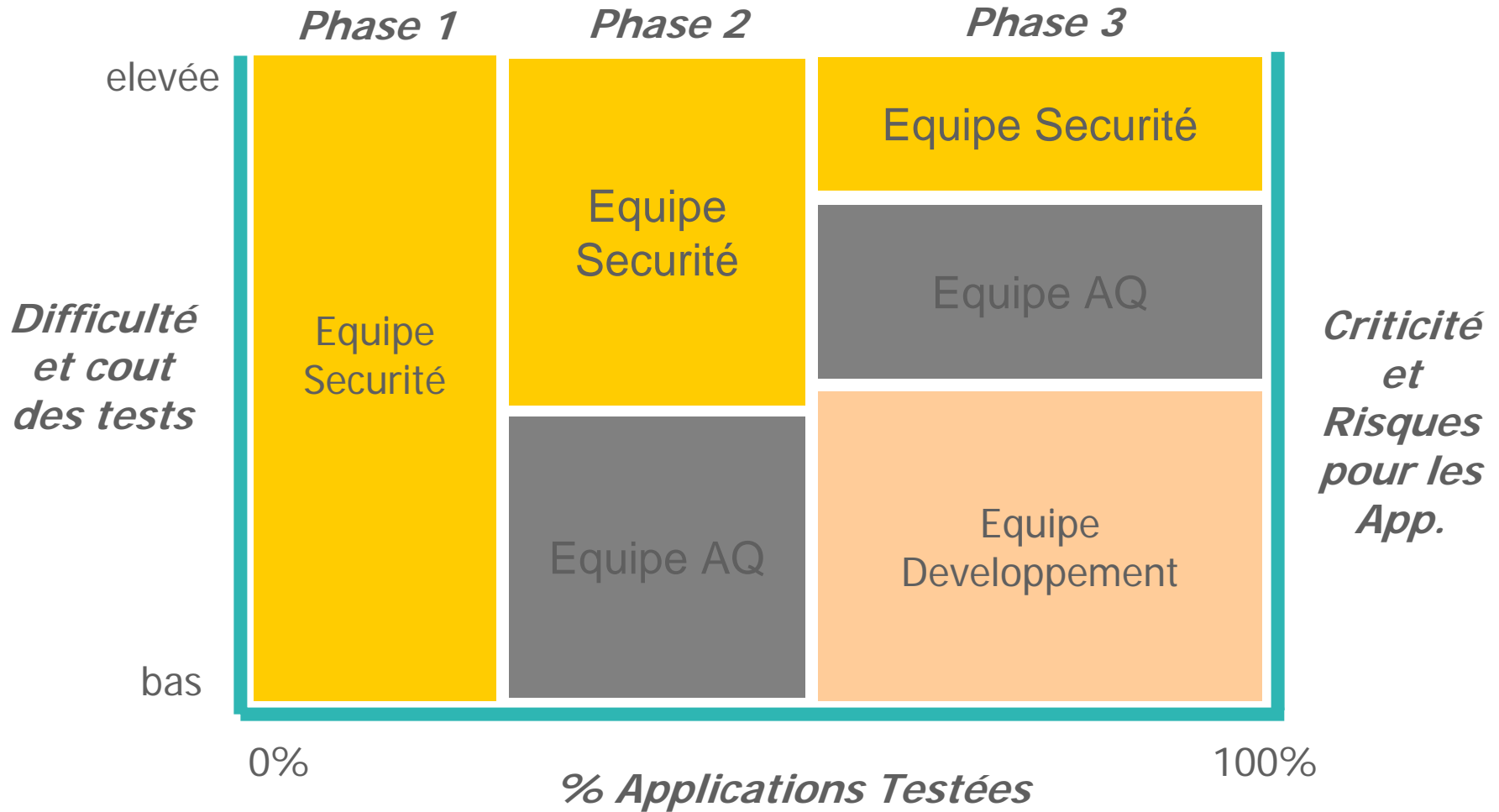




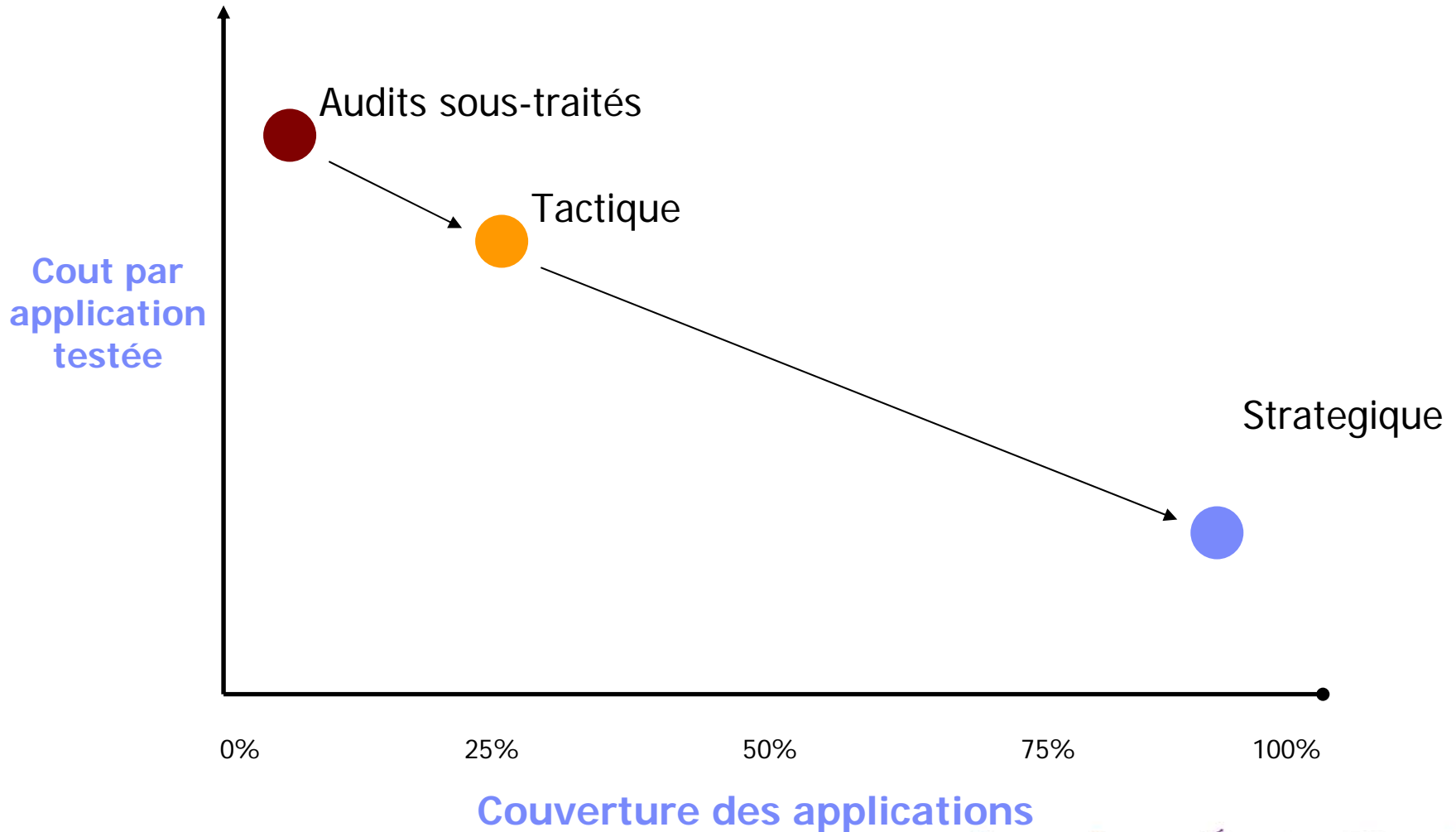
# Modèle de maturité de la sécurité applicative



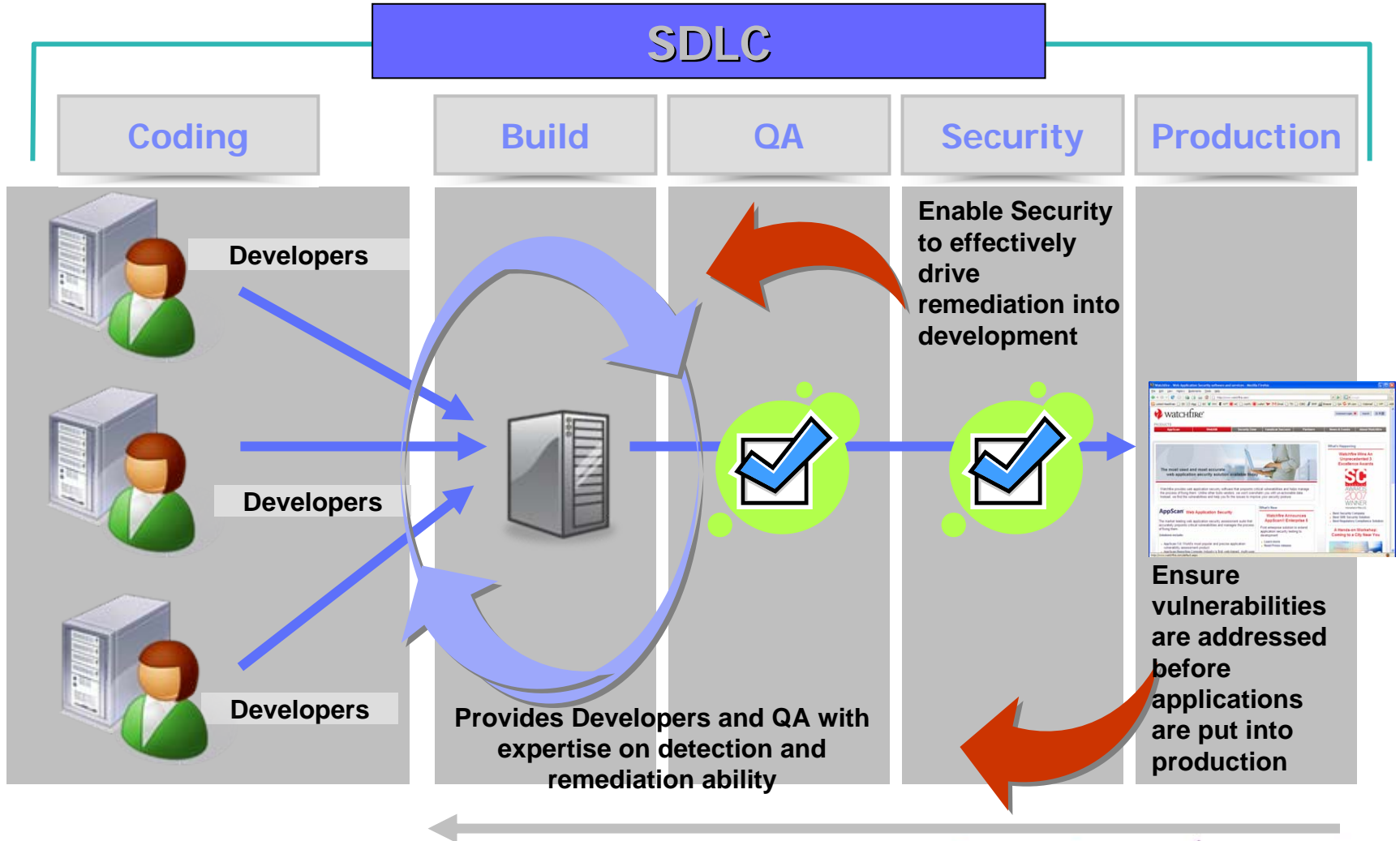
# Modèle de maturité de la sécurité applicative



# Reduire les couts, Etendre la couverture



# Sécurité et conformité dans le processus de devp.



Application Security Testing Maturity

# 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

The screenshot displays the Watchfire AppScan interface. The main window shows a scan of 'My Application' (54) at 'http://demo.testfire.net/'. A list of security issues is shown, including Blind SQL Injection (4), Cross-Site Scripting (1), Format String R (1), HTTP Respons (1), Session Not Inv (1), SQL Injection (1), and XPath Injection (1). A 'Defect Details' window is open, showing the following information:

- Credentials:** Username: admin, Password: [redacted]
- Defect Details:**
  - Summary: SQL Injection in http://revelation/acmehackme/bank/login.aspx (Parameter passw)
  - id: [redacted]
  - State: [redacted]
  - Project: [redacted]
  - Keywords: [redacted]
  - Severity: 1-Critical
  - Symptoms: [redacted]
  - Priority: solve Immediately (dropdown menu open showing options: 1-Resolve Immediately, 2-Give High Attention, 3-Normal Queue, 4-Low Priority)
  - Owner: engineer
- Description:**
  - SQL Injection
  - Application-level test
  - WASC Threat Classification: Command Execution: SQL Injection
  - Security Risk: It is possible to view, modify or delete database entries and tables
- Attachments:**
  - Open, Edit, Remove, Add Attachment...
  - Advisor.html, FixRec.html, Variant1-Uri..., Variant1-1es..., Variant2-Uri..., Variant2-1es..., Variant3-Uri...

Buttons at the bottom of the Defect Details window include Cancel and Log Defect.

# Détecter et corriger au plus tôt les vulnérabilités applicatives

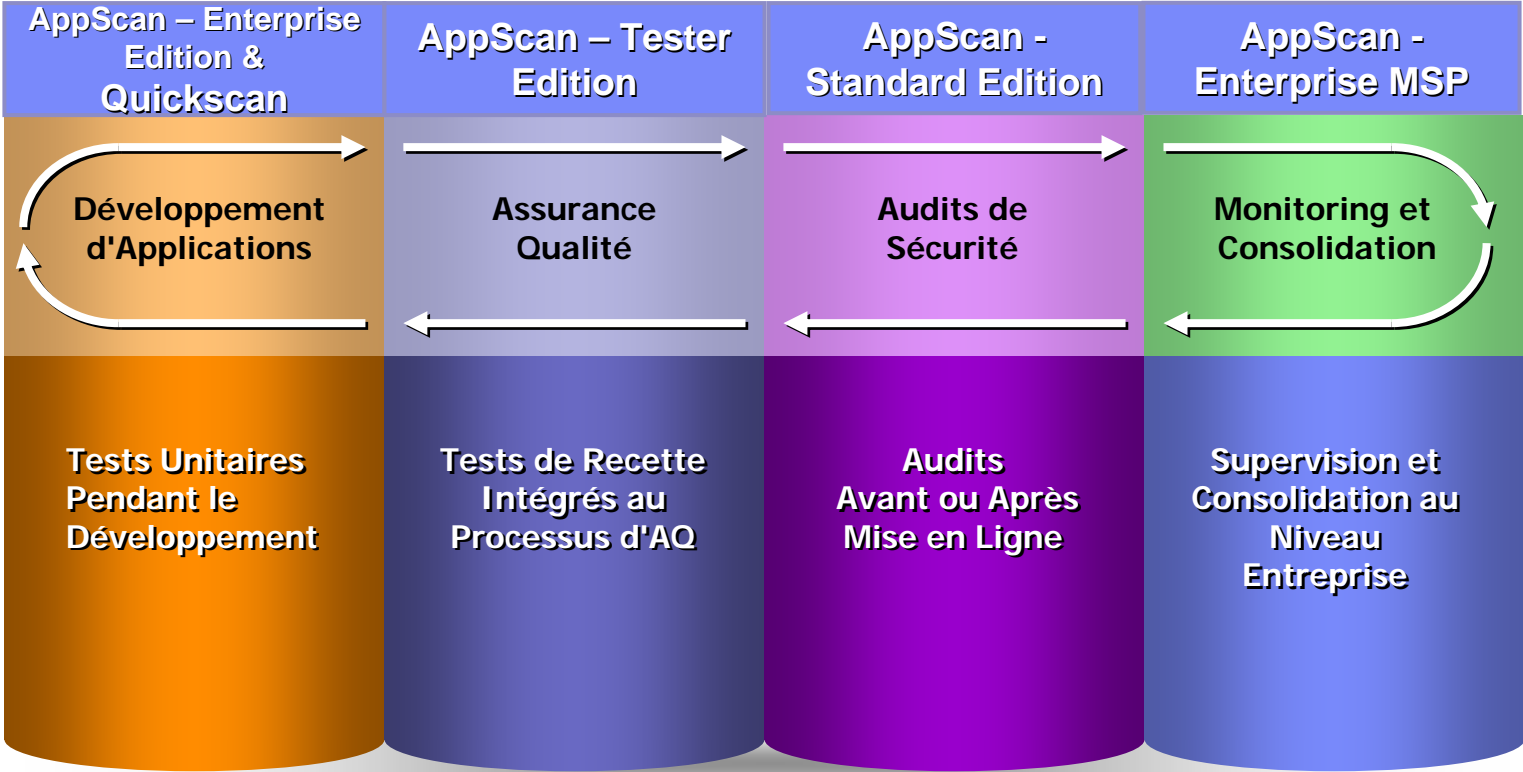
- AppScan permet au développeur de tester ses transactions et services dès leur mise au point, depuis son environnement de travail
- Il peut être intégré dans **Eclipse**, **Websphere**, **JBuilder** ou **Visual Studio.Net**
- AppScan effectue les tests applicatifs et offre des explications et aides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

The screenshot shows the Microsoft Development Environment (MSDE) with the AppScan 7.5 Demo Scan window open. The AppScan window displays a list of security issues for 'My Application' (53) and a detailed view of a 'Blind SQL Injection' issue. The 'Fix Recommendation' section provides general advice on sanitizing user input and lists characters to filter out: [1] pipe sign, [2] ampersand sign, and [3] semicolon sign.

# Famille des produits Rational AppScan

## Rational AppScan Enterprise

La Sécurité des Applications Web à travers tout leur Cycle de Vie





# AppScan Enterprise

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

The screenshot displays the Watchfire AppScan Enterprise web interface. At the top, it shows the user 'Jim (security analyst)' and navigation links for 'Jobs & Reports' and 'Administration'. The main content area is titled 'Application Dashboard - Graphical View' and includes several charts and reports:

- Issue Severity History:** A line chart showing the number of issues over time, categorized by severity: High (red), Medium (orange), Low (yellow), and Information (white).
- Issue Management History:** A stacked area chart showing the status of issues: Fixed (green), In Progress (red), Reopened (orange), Open (yellow), and Active (white). The current active count is 509.
- Issue Severity by Report Pack:** A horizontal bar chart showing the distribution of issue severities across different report packs.
- WASC Threat Classification:** A pie chart showing the distribution of threats across categories: Authentication, Authorization, Client-side Attacks, Command Execution, Information Disclosure, and Logical Attacks.

On the left side, there is a 'Folders' tree view for 'Acme Hackme Bank' containing subfolders for 'Analysts' (Frank, Jim) and 'Developers' (Andrew, Jennifer, Rick). A 'Recently Viewed' list is also visible at the bottom left.



# + de 800 Entreprises font Confiance à Watchfire

9 des 10 1 <sup>ères</sup> Banques	8 des 10 1 <sup>ères</sup> Sociétés High-Tech	7 des 10 1 <sup>ères</sup> Groupes Pharmaceutiques	Plusieurs Grandes Administrations

## FRANCE:

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

- Sur [www.watchfire.com](http://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 gratuitement :**

**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 ...



**You're invited**

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



## 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](#)

© Copyright IBM Corporation 2007. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, the on-demand business logo, Rational, the Rational logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

