Tendances Logicielles

PORTE 04

Rational

Eliminer les risques liés aux failles de sécurité dans les applications Web avec Rational AppScan

Kamel Moulaoui

1er et 2 octobre 2007

IBM

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

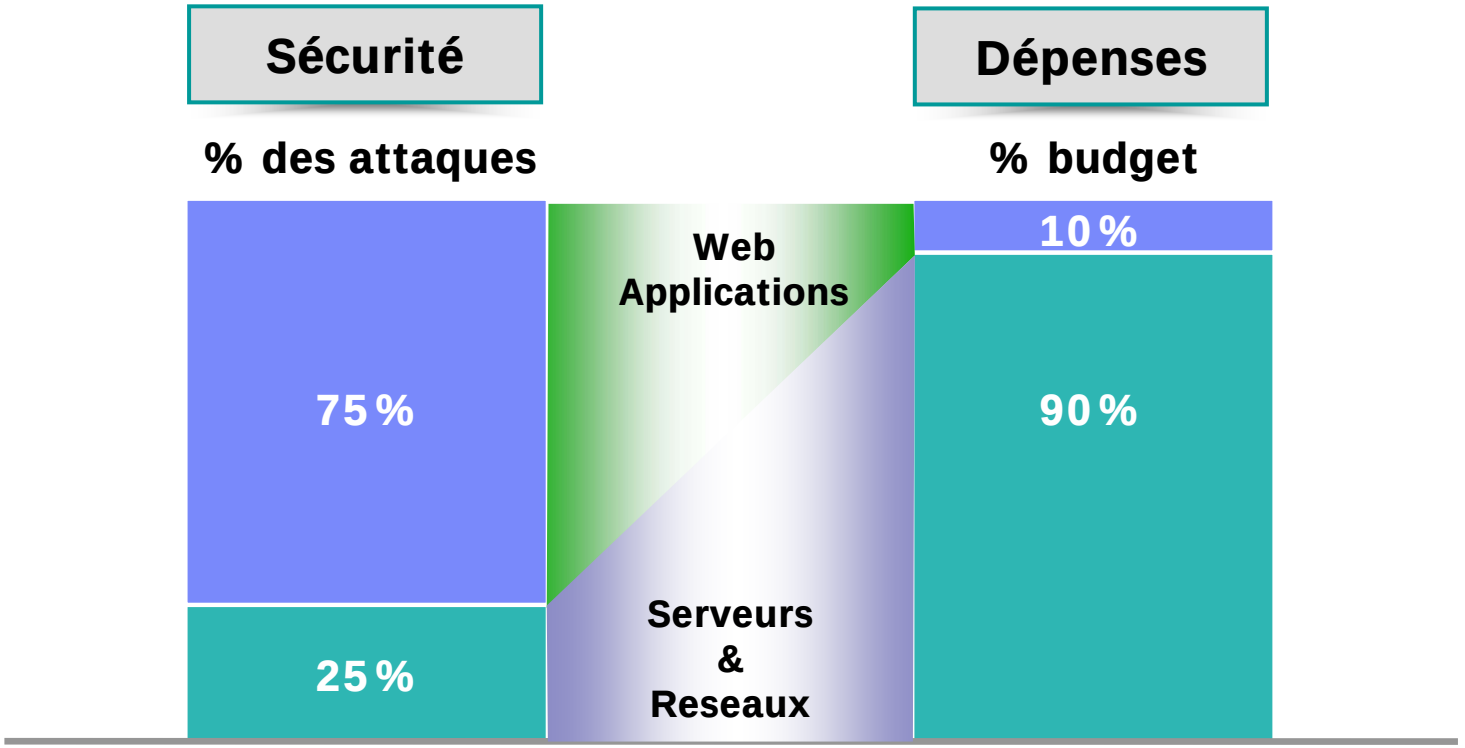
Pourquoi la sécurité applicative est une haute priorité ?

- **Les Applications Web sont la cible #1 des hackers:**
  - 75% des attaques concernent la couche application (Gartner)
  - XSS et SQL Injection sont #1 et #2 des vulnérabilités reportées (Mitre)
- **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:**
  - Données clients, Cartes de crédit, vol et usurpation d'identités, fraude, etc.
- **Exigences de conformité:**
  - Payment Card Industry (PCI) Standards, GLBA, HIPPA, FISMA etc.

Le coût de la violation de la sécurité applicative

- L'attention des médias se traduit
  - Dommages causés aux marques
  - Méfiance des investisseurs (cours de l'action chahuté)
- Coûts en service de communication/de suivie
- Honoraires
- Pénalités
- Audits
- Procès de clients
- Perte de clients

La sécurité et les dépenses ne sont pas équilibrées



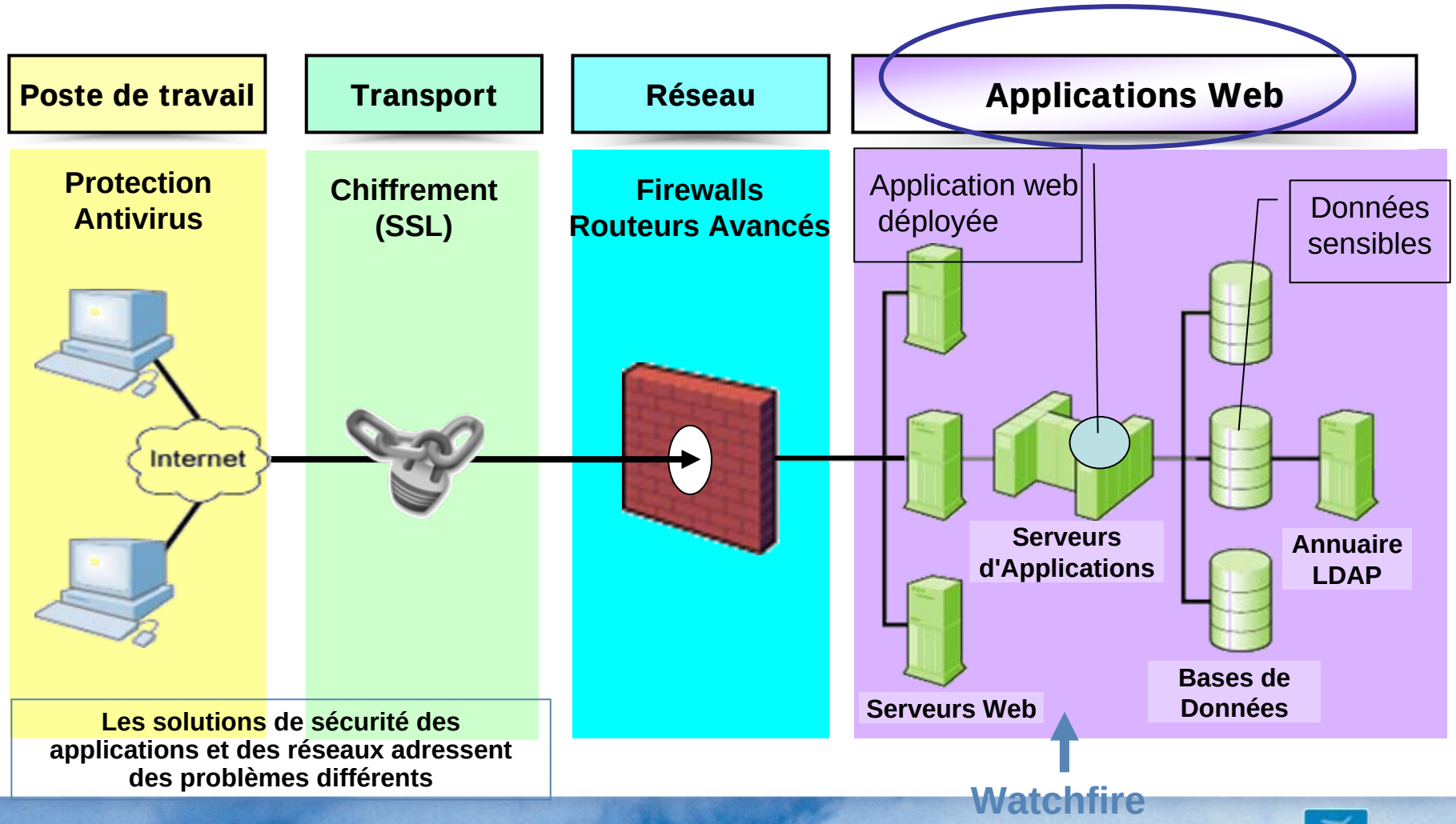
75% Des attaques sur la sécurité de l'information sont dirigées vers la couche application web

2/3 De toutes les applications Web son vulnérables

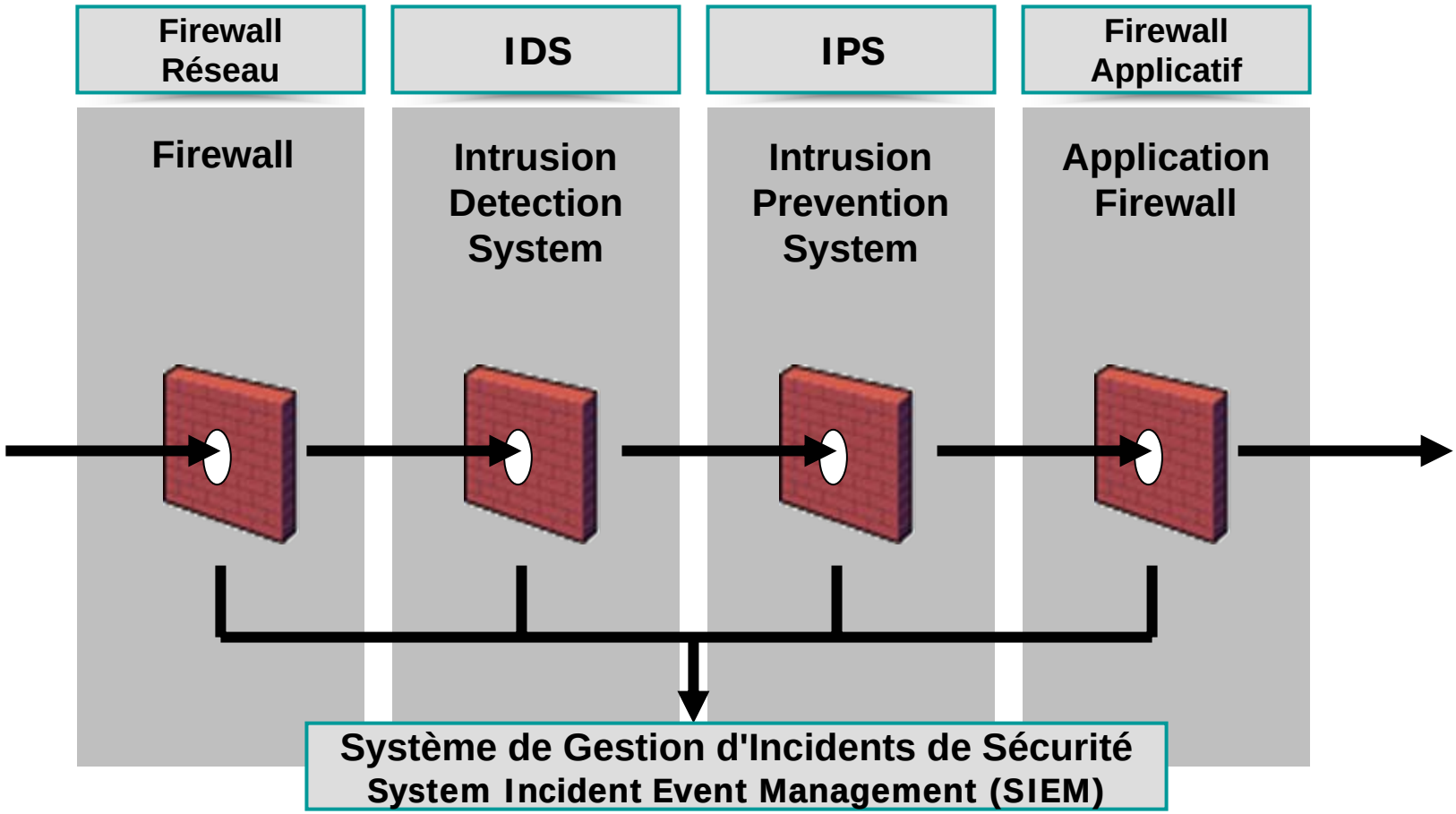
Gartner

Sources: Gartner, Watchfire

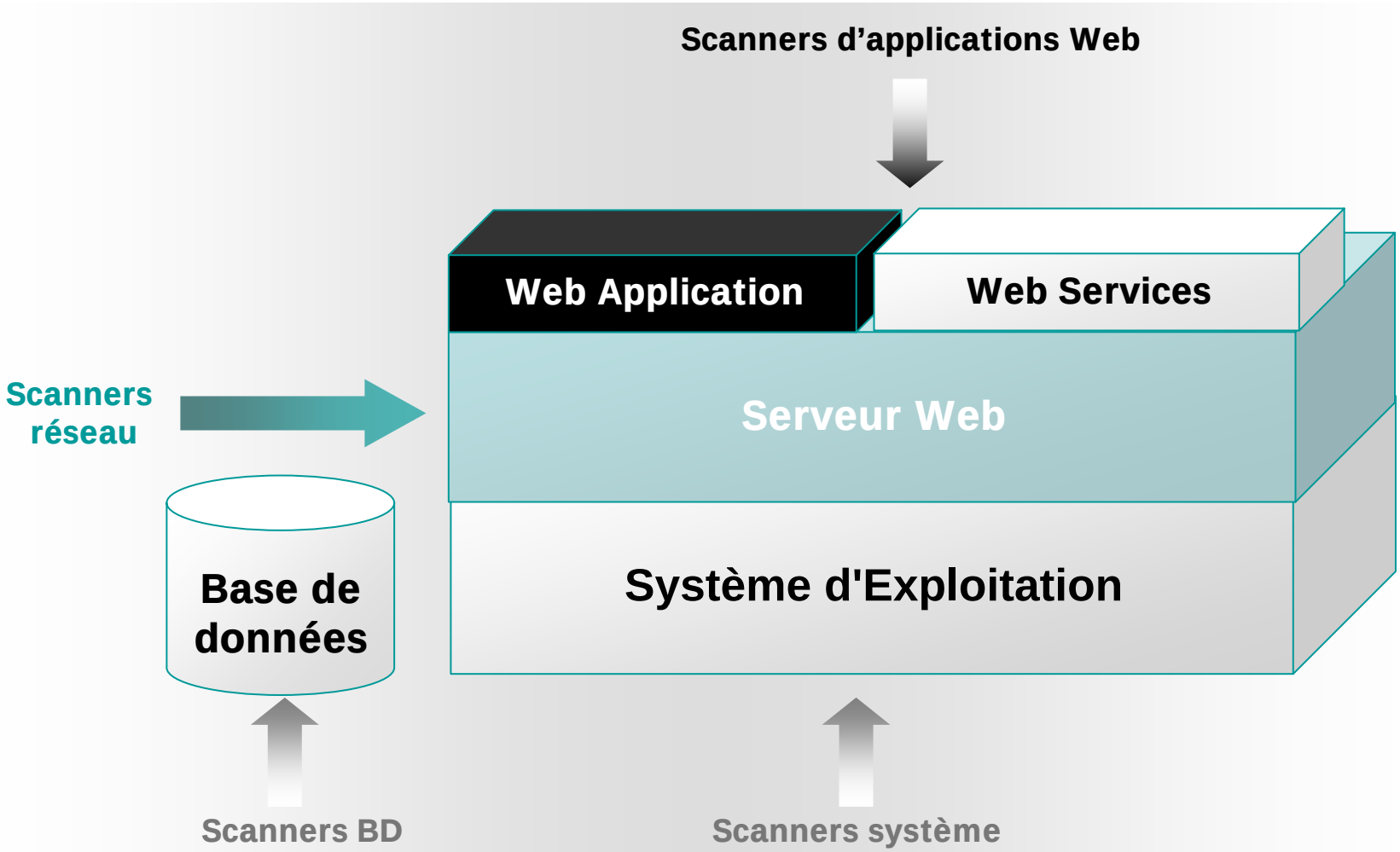
Architecture Globale d'une Application Web Sécurisée



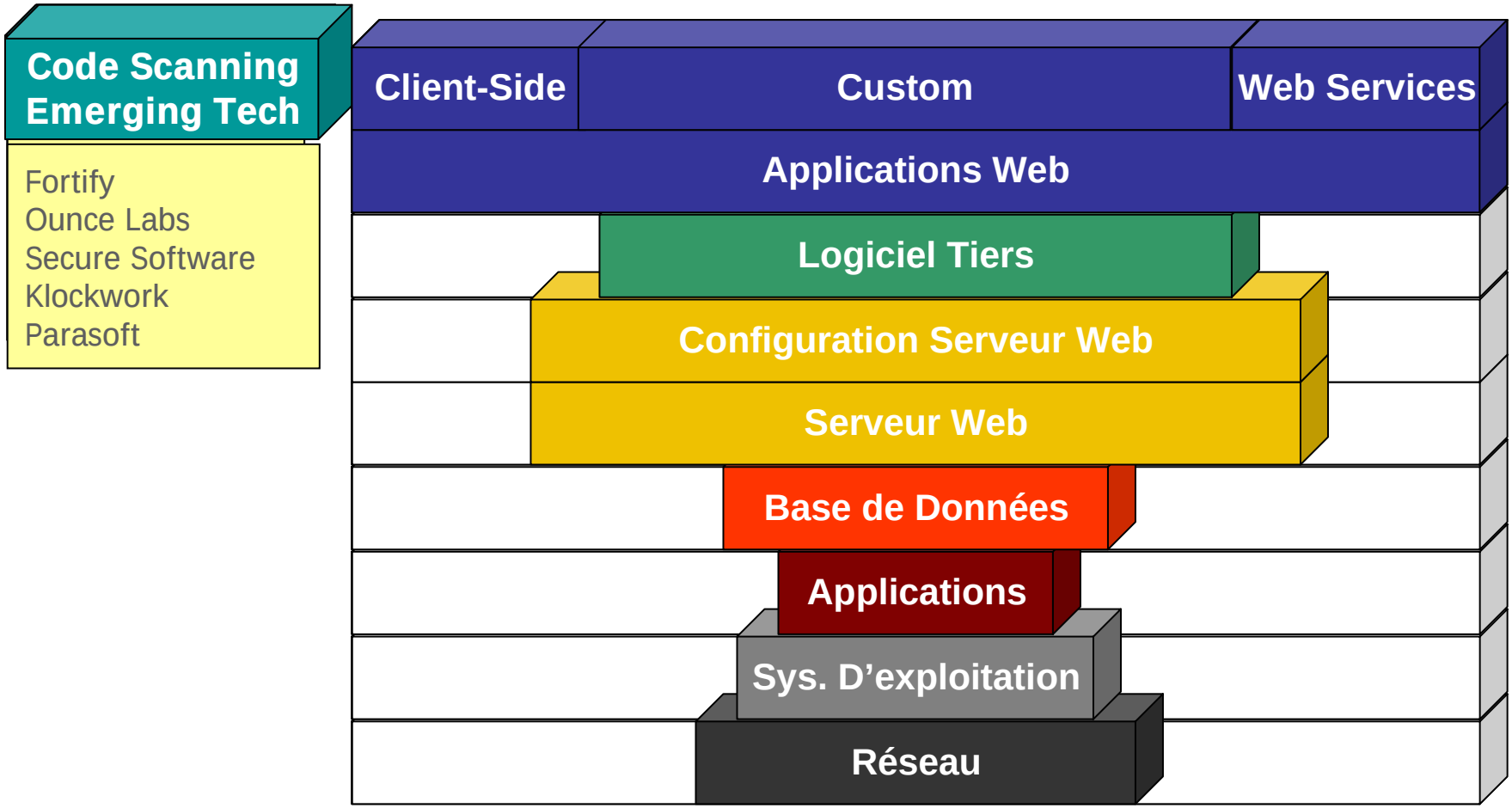
Protections Réseau pour Applications Web



Environnement d'une application Web



Où sont les Vulnérabilités?



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.

Watchfire: une compagnie IBM, intégrée au brand Rational

Watchfire fournit des solutions de test de vulnérabilité et de conformité des applications web pour aider les entreprises à **réduire les risques et les coûts** associés aux infractions en ligne de sécurité et de conformité.

Watchfire

La société

- Précurseur dans les domaines de la qualité, conformité et sécurité des applications Web (depuis + 10 ans) .
- Leader sur le marché selon Gartner & IDC
- Le plus grand nombre de solutions déployées auprès des clients
  - Notoriété acquise par l'expérience dans la sécurité applicative

La Technologie

- Le scanner le plus complet pour la couverture des applications Web
- Détecte la plupart des vulnérabilités graves
- Le plus petit taux de faux positif du marché
- Facilité d'exploitation et de communication des résultas pour les non experts de la sécurité.
- Interface Web pour une exploitation et un déploiement simplifiés
- Formation et service d'accompagnement
  - Processus basé sur les meilleures pratiques pour auditer et corriger les anomalies

+ 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	
citi	Cisco Systems	Novartis	
AXA Financial Protection	intel	AstraZeneca	
Fidelity	DELL	Abbott Laboratories	
SunTrust	IBM	Aventis	
Liberty Mutual	SONY		
Sovereign Bank	Adobe	Roche	
	Analog Devices	Genentech	United States Postal Service

AppScan: #1 des scanners des Vulnérabilités Applicatives (*)

(*) **Gartner** - Application Security Vulnerability Scanning, May 2006, **IDC** - Application Security Vulnerability Management, January 2006

Rational AppScan

- Qu'est ce que Rational AppScan ?
  - Rational 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 Rational 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)

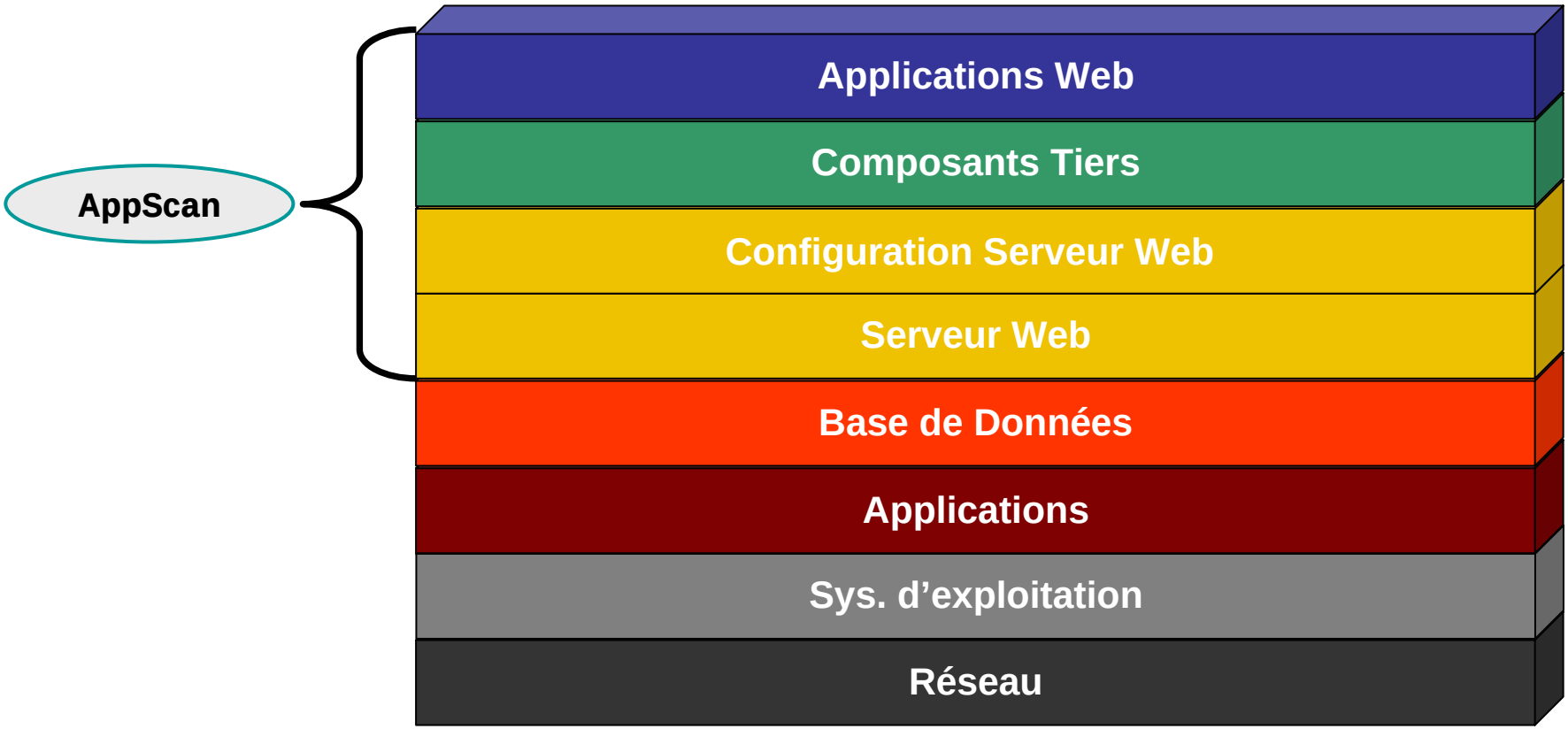
Points Forts & Différentiateurs

- Universalité & Puissance du Scanner
  - Pas de limitations technologiques ou conceptuelles: pratiquement toute application web peut être testée correctement, avec un effort minimal
- Etendue des Tests et Elaboration de Stratégies
  - Très large collection de vulnérabilités applicatives, constamment mise à jour (R&D+veille) et facilement utilisable lors d'un audit particulier
- Exploitation et Validation des Résultats
  - Exploration, compréhension et vérification des résultats sont facilitées par une IHM intuitive et les aides à la correction sont très développées
- Rapports de Sécurité et de Conformité
  - Rapports adaptés à chaque intéressé par la sécurité dans l'entreprise et + de 30 rapports de conformité, adressant différents risques métier
- Exploitabilité Accrue
  - Des fonctions, mécanismes et outils complémentaires qui facilitent l'adoption de l'outil et son usage au quotidien

IBM Rational AppScan: Détection des Vulnérabilités

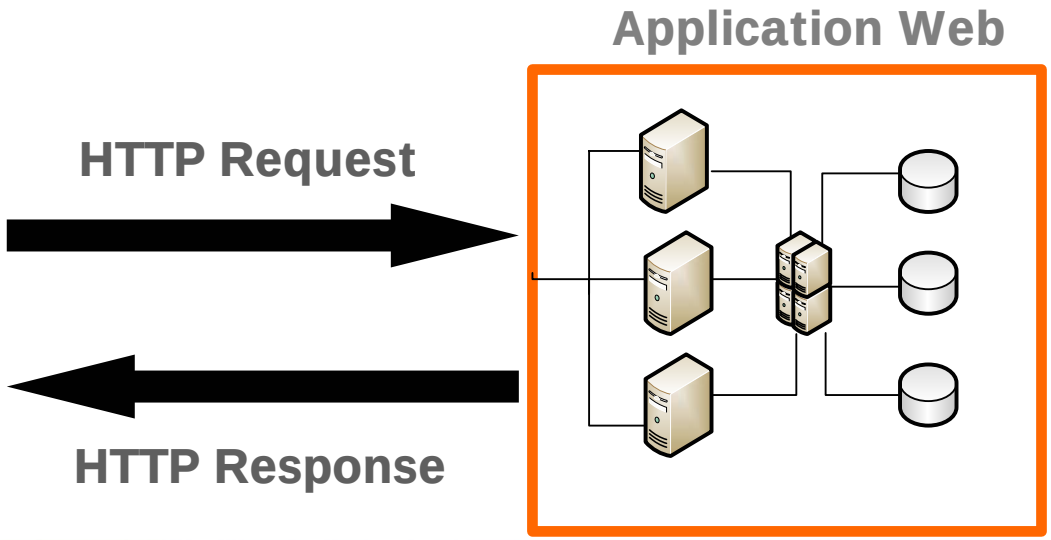
- Rational AppScan simule l'exécution des attaques suivantes:
  - cross-site scripting
  - HTTP response splitting
  - parameter tampering
  - hidden field manipulation
  - backdoor/debug options
  - stealth commanding
  - forceful browsing
  - application buffer overflow
  - cookie poisoning
  - third-party misconfiguration
  - known vulnerabilities
  - HTTP attacks
  - SQL injections
  - suspicious content
  - XML/SOAP tests
  - content spoofing
  - Lightweight Directory Access Protocol (LDAP) injection
  - XPath injection
  - session fixation

Les composants testés par Rational AppScan

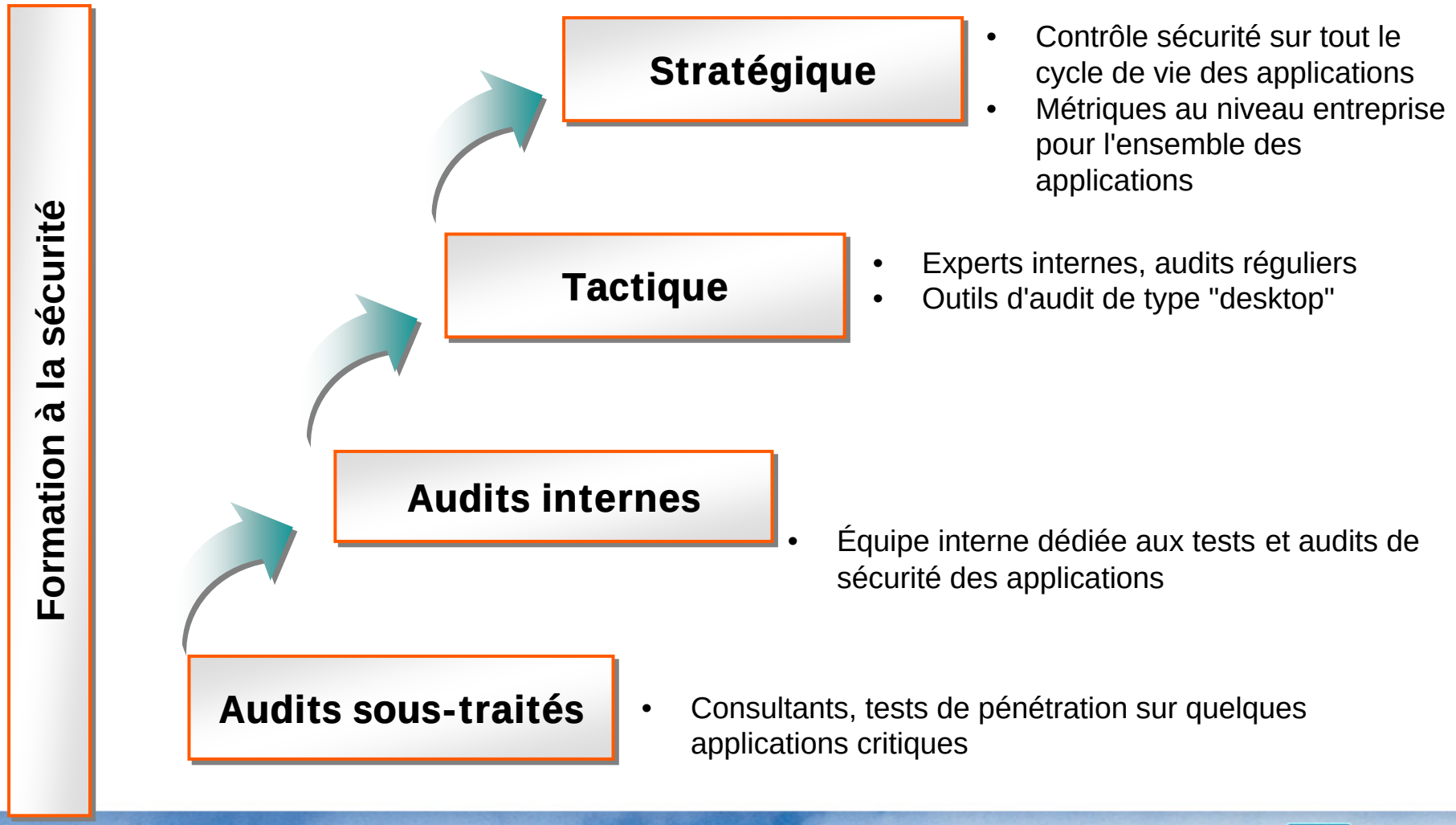


Rational AppScan: Principe de fonctionnement

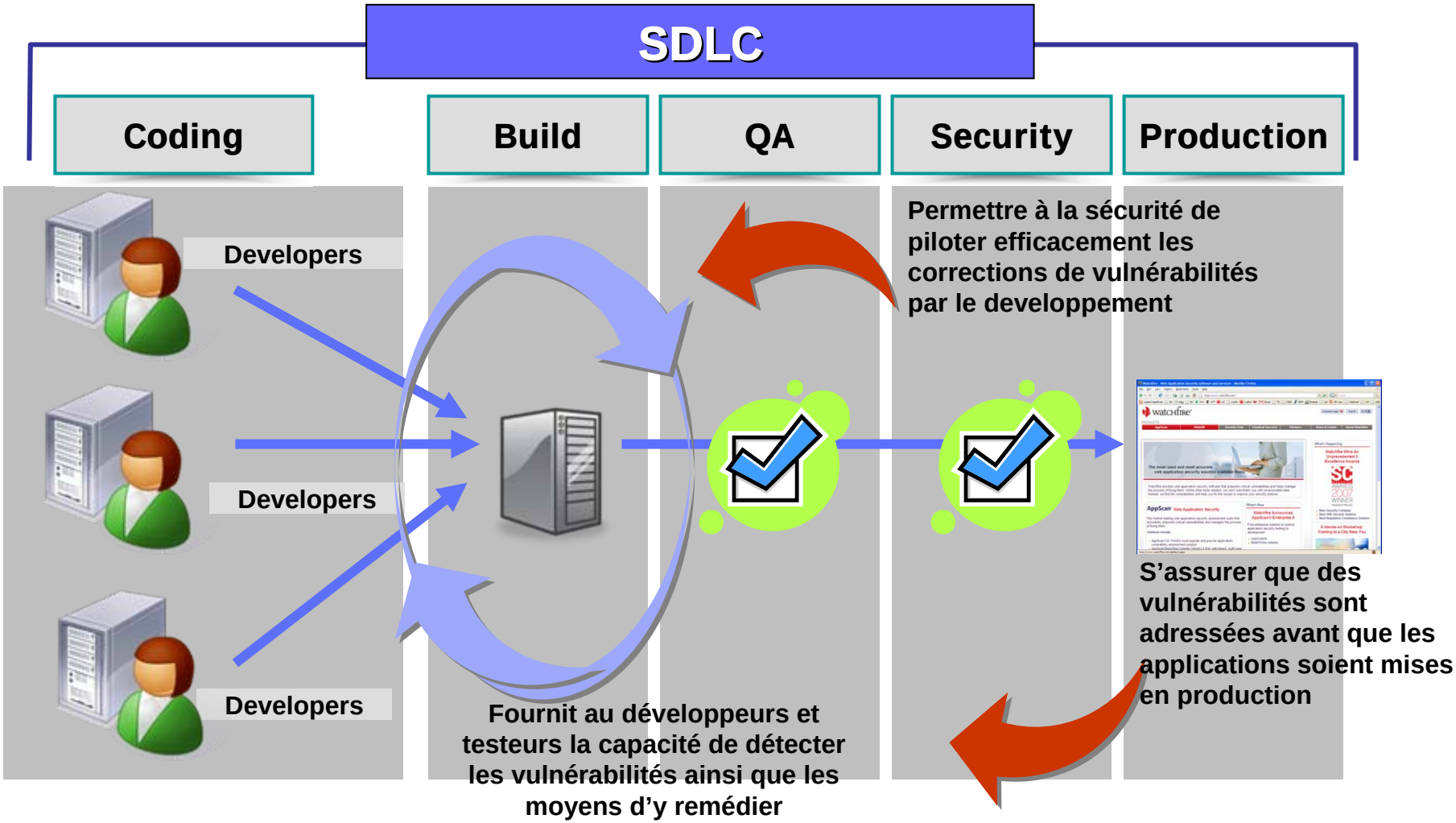
- Aborde l'application comme une boite noire
- Parcourt l'application web et construit un modèle du site
- Détermine les vecteurs d'attaque basés sur la politique choisie du test
- Teste en envoyant des requêtes HTTP modifiées à l'application et en examinant les réponses HTTP selon les règles de validations.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



Modèle de maturité de la sécurité applicative

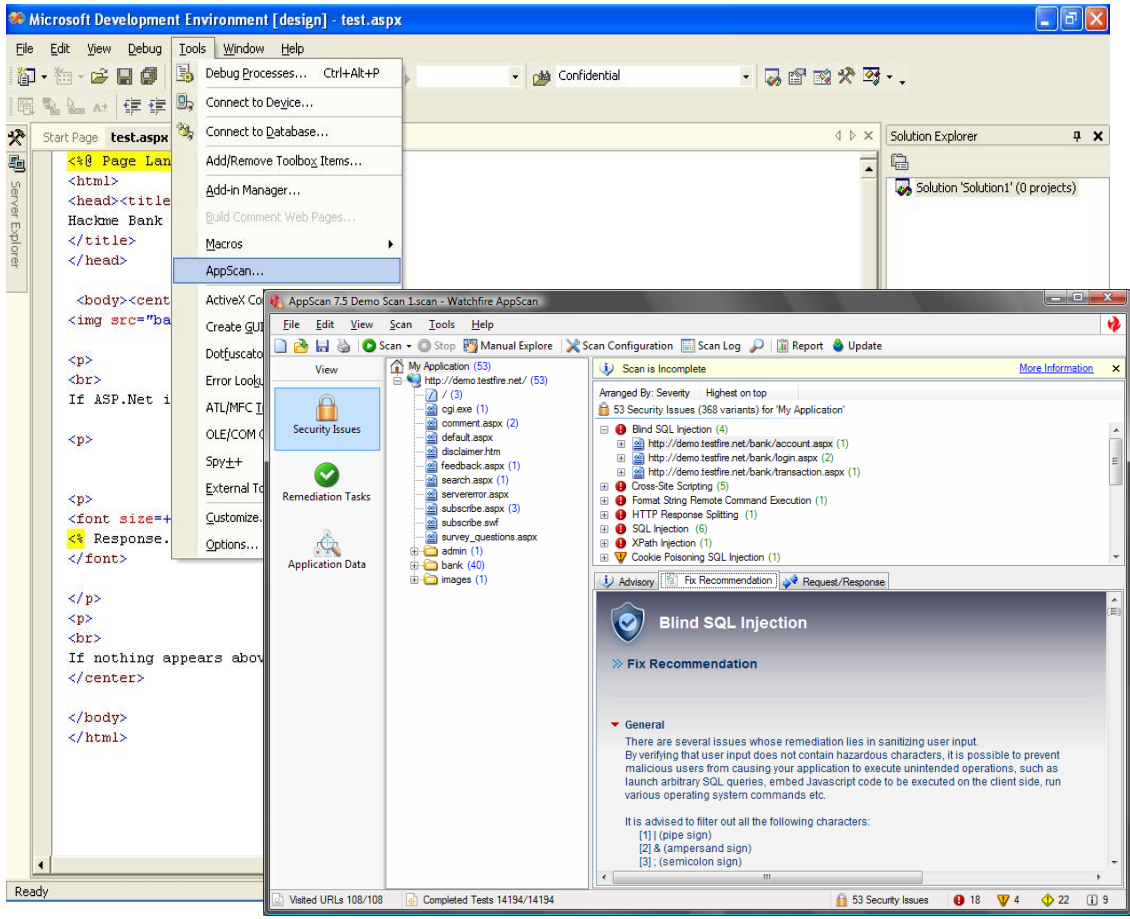


Sécurité et conformité à travers tout le cycle de vie



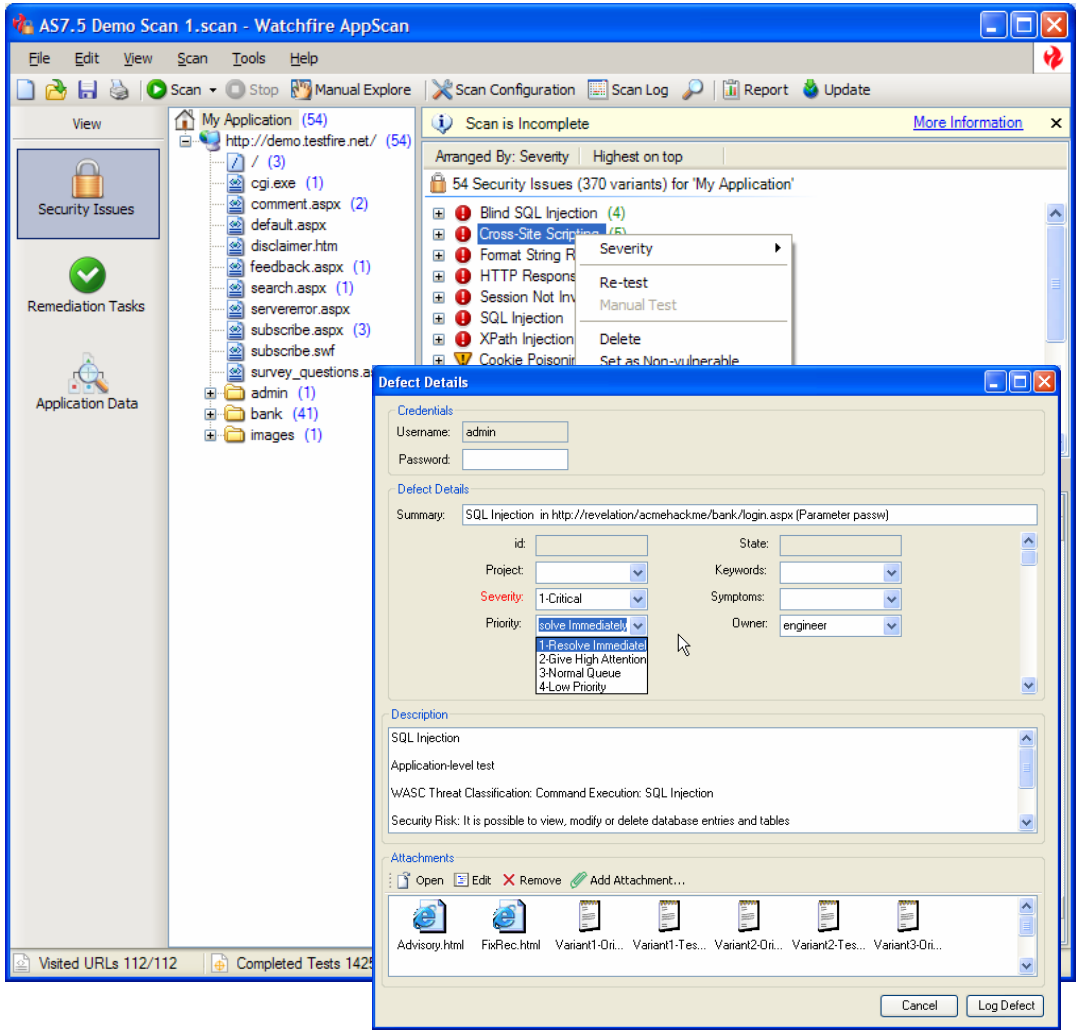
Détecter et corriger au plus tôt les vulnérabilités applicatives

- 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

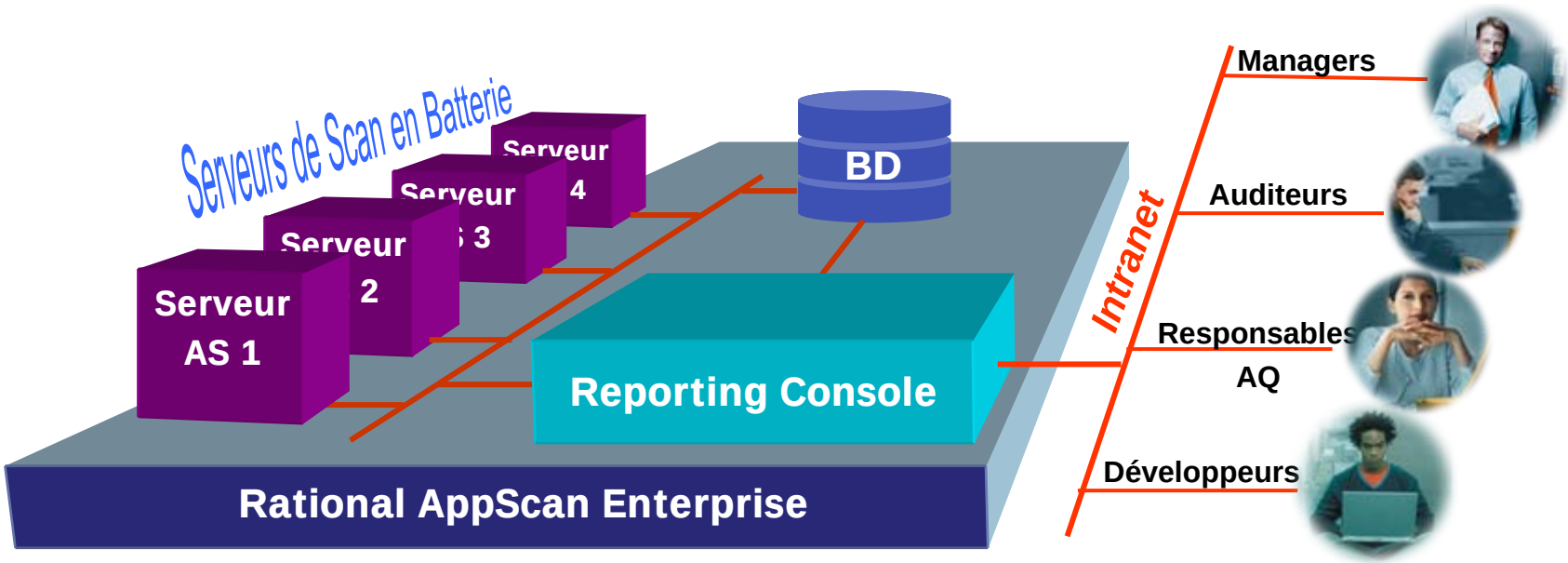


Intégrer la sécurité dans le processus d'Assurance Qualité

- 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

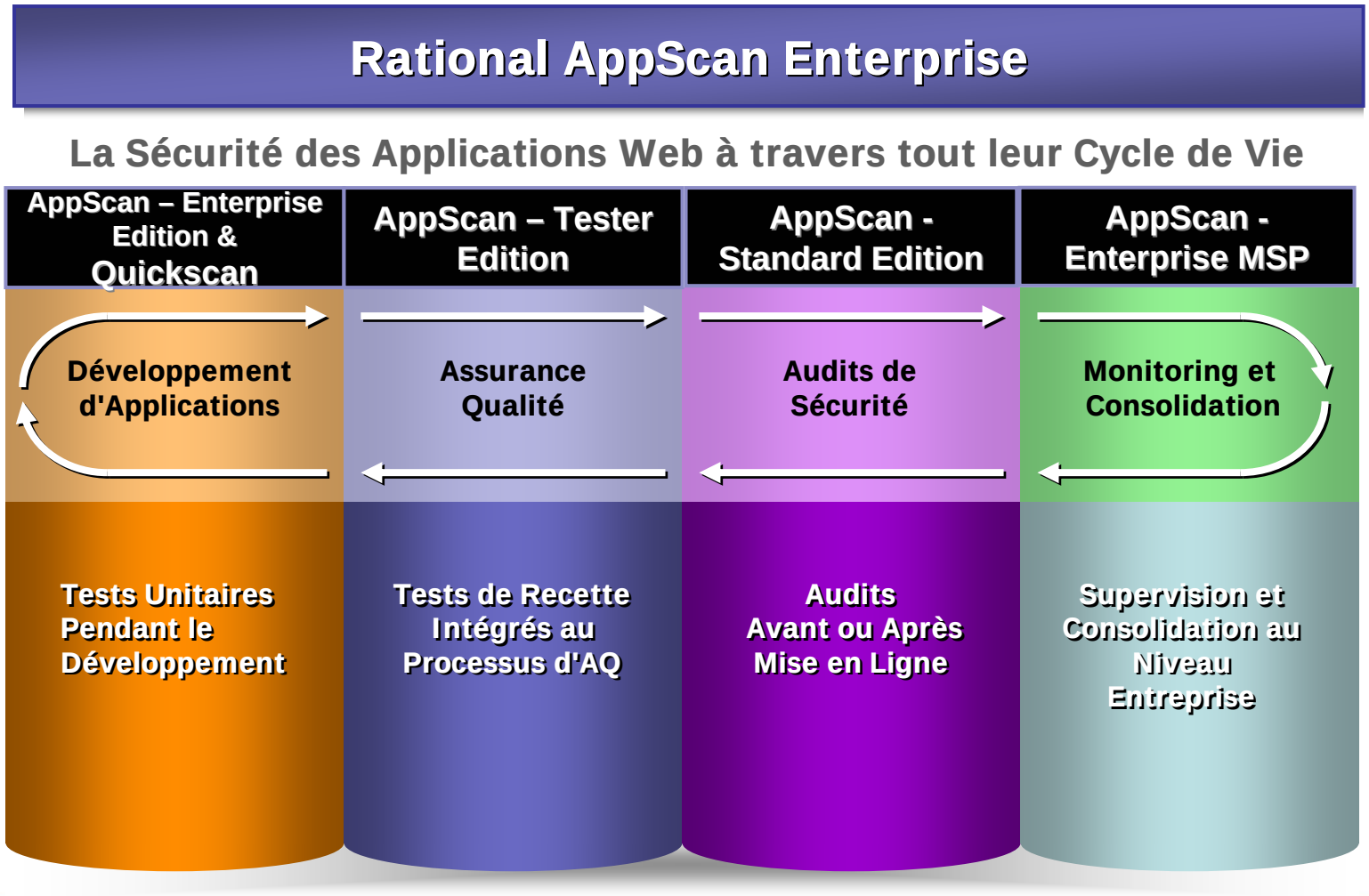


Faciliter la généralisation et l'exploitation de Rational AppScan au niveau de l'organisation



- Puissance d'analyse pratiquement illimitée
- Exploitation et déploiement simplifiés: plus de Desktops à gérer

Famille des produits Rational AppScan




DEMO


Questions

TEC - Technical Exploration Center - @ Paris

Accélérer le cycle de découverte des logiciels IBM

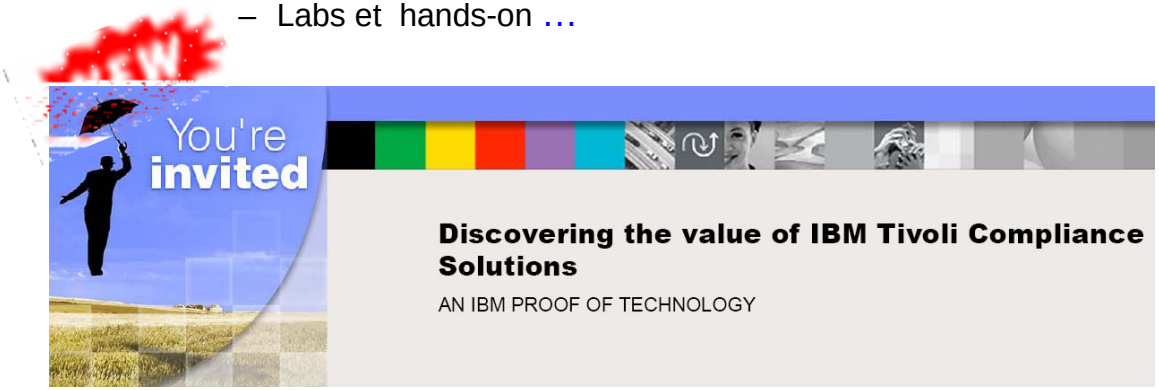
Les ressources hardware et software du TEC
à Noisy-Le Grand / Marne La Vallée
sont disponibles <u>gratuitement</u> :

« 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



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