IBM

Tom Pertsekos

Sécurité applicative Web : gare aux fraudes et aux pirates !

TENDANCES LOGICIELLES D'ÉTÉ 2008

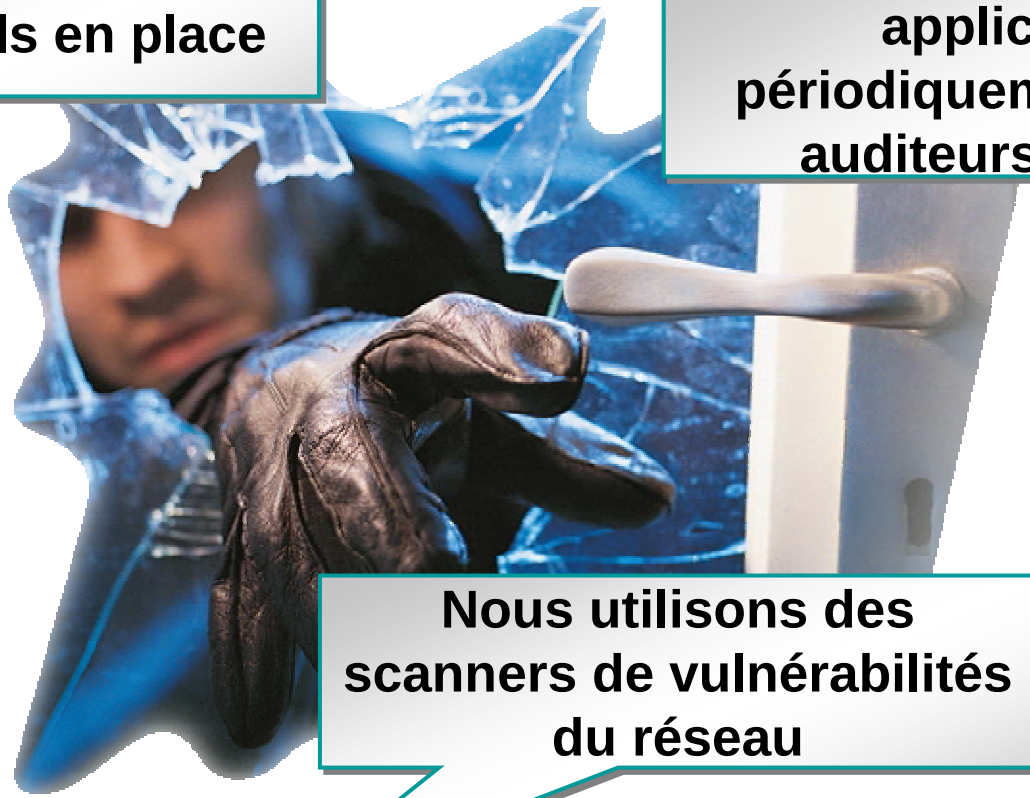
SESSION SPÉCIALE GESTION DES RISQUES OPÉRATIONNELS

Sécurité

Le mythe : « Notre site est sûr »

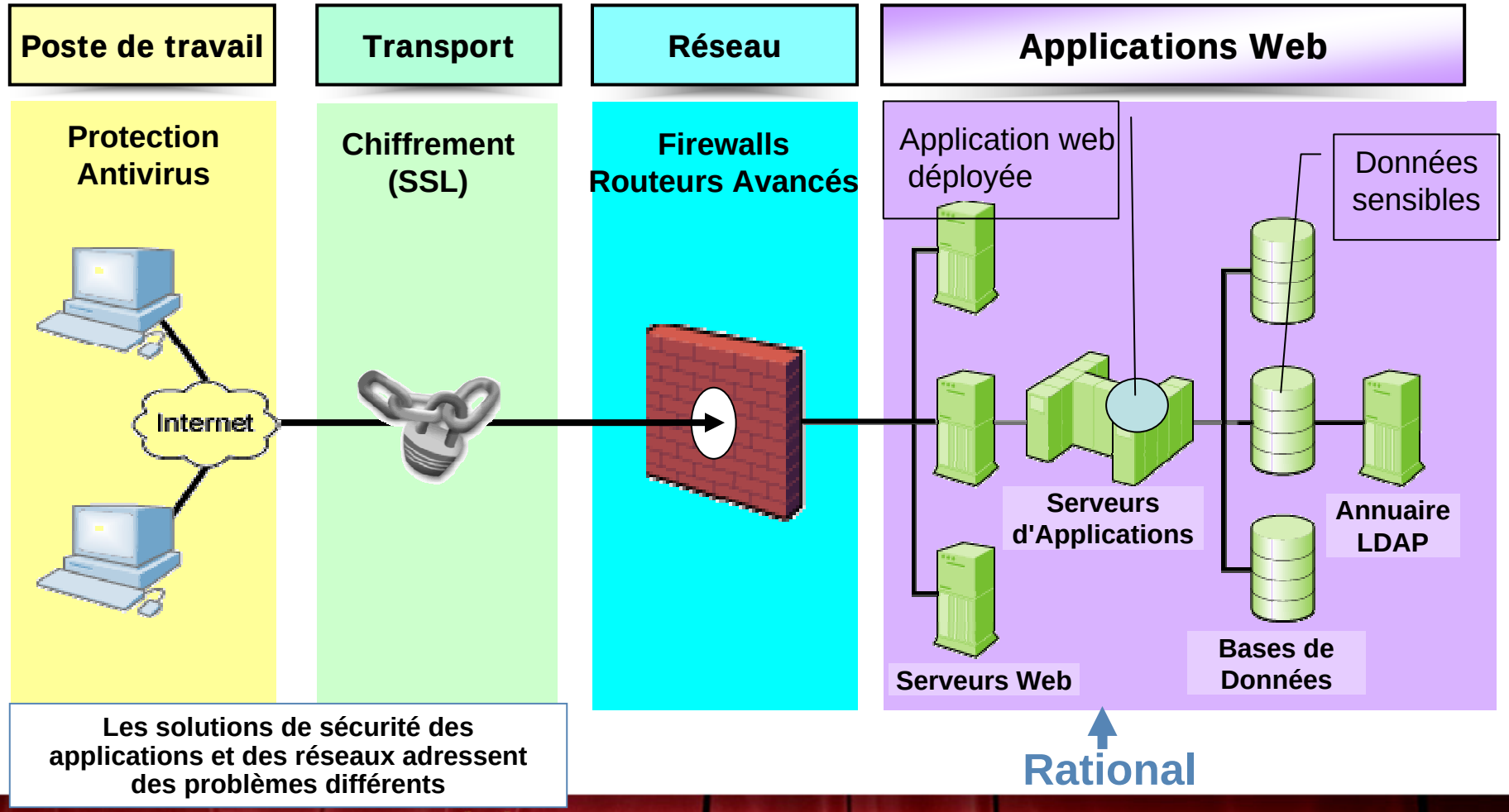
Nous avons des Firewalls en place

Nous auditons nos applications périodiquement par des auditeurs externes



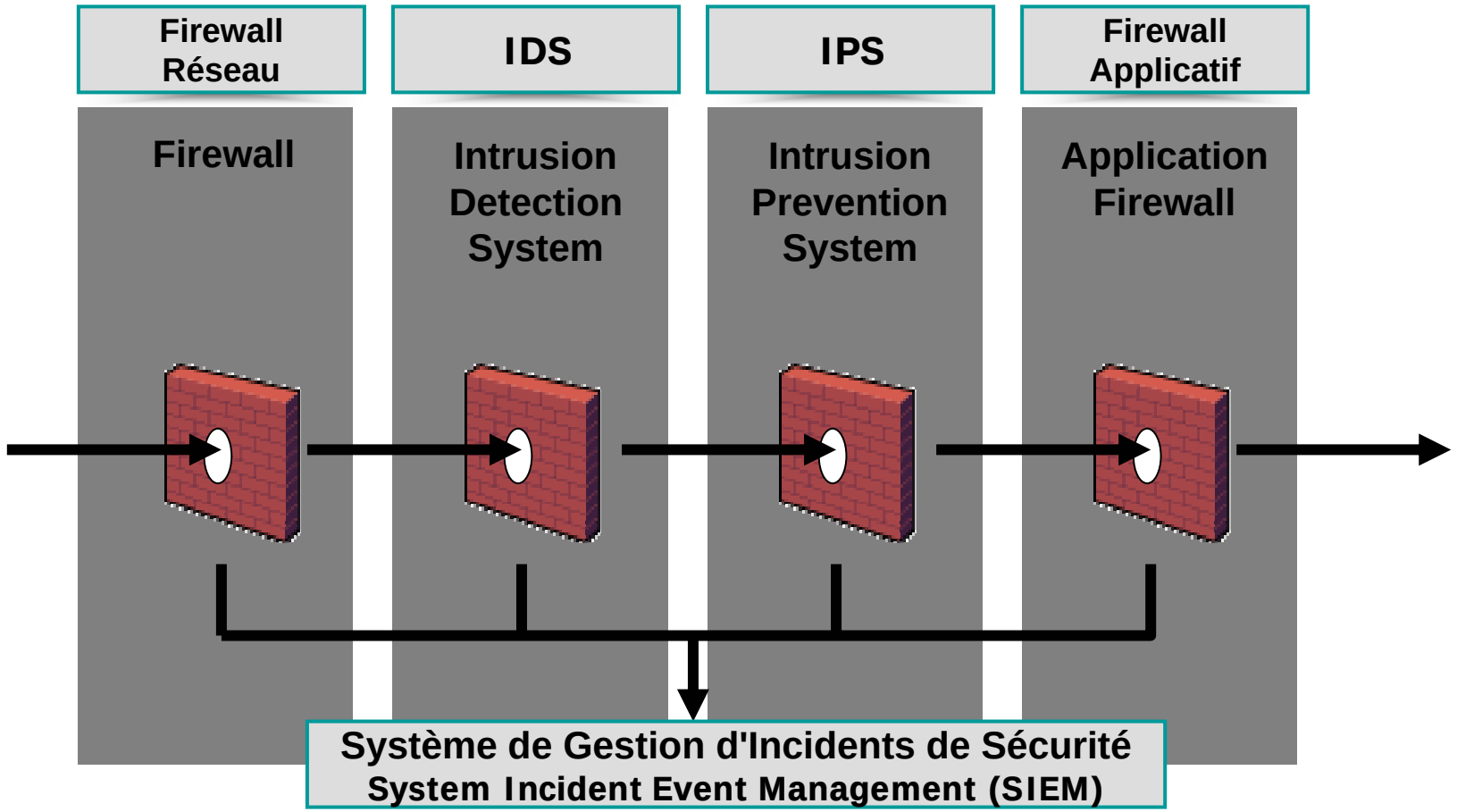
Nous utilisons des scanners de vulnérabilités du réseau

Architecture Globale d'une Application Web Sécurisée



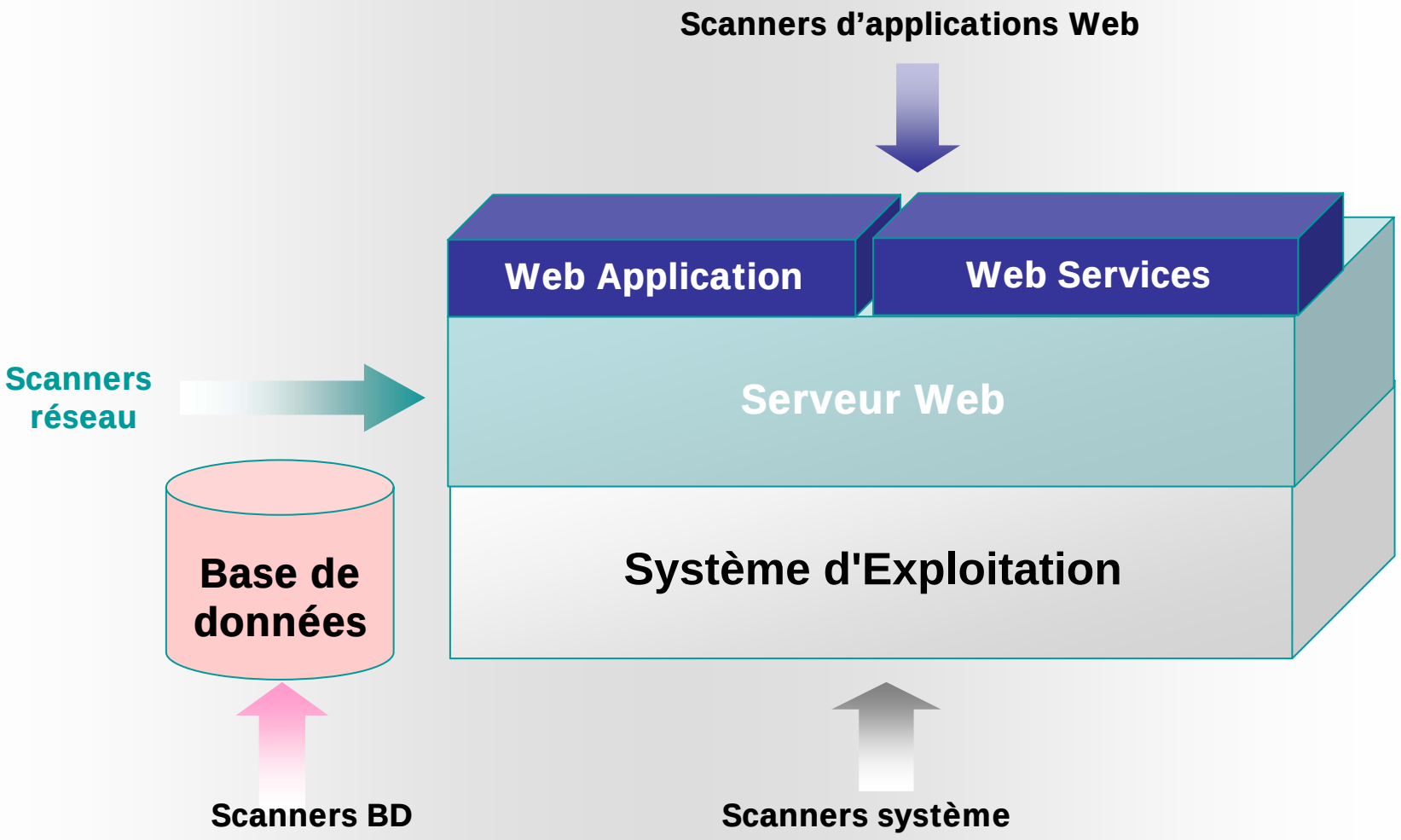
Sécurité

Protections Réseau pour Applications Web



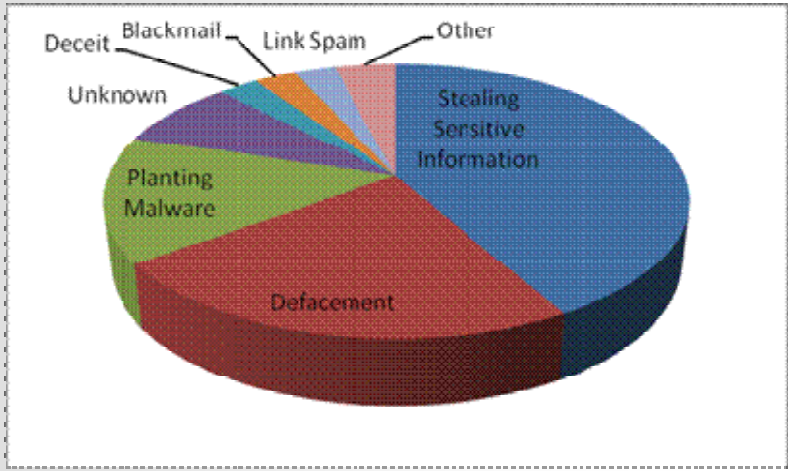
Sécurité

Environnement d'une application 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.




DEMO

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%

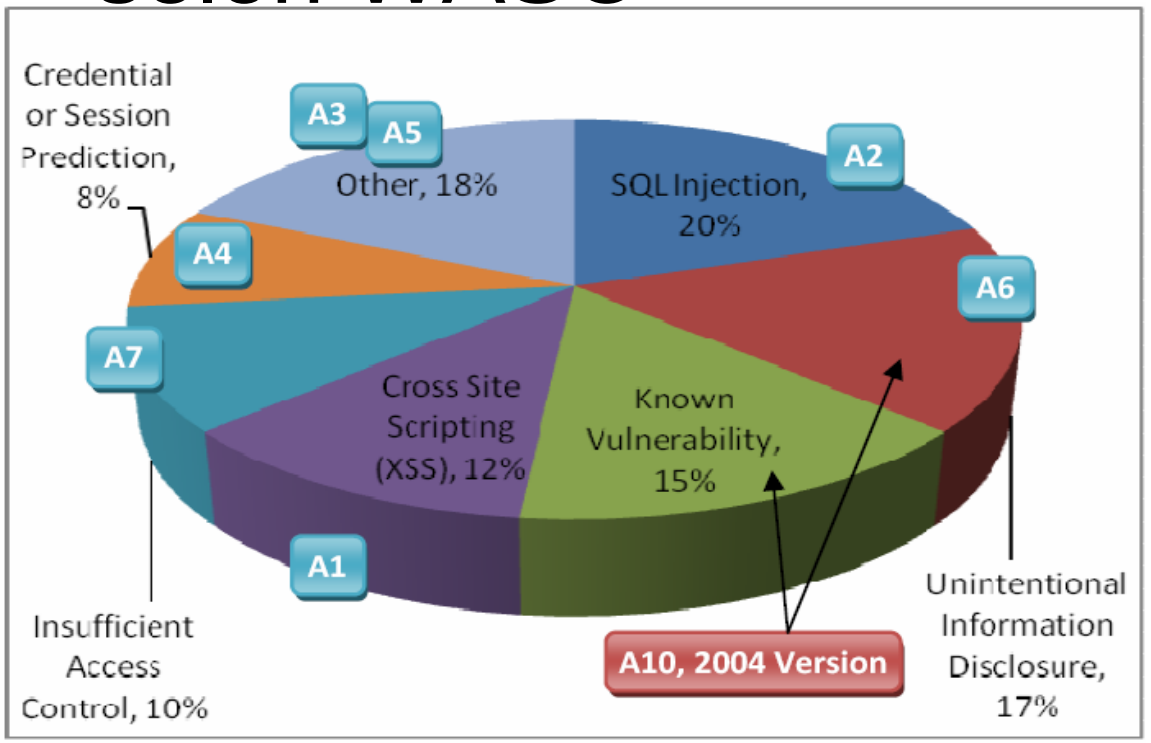


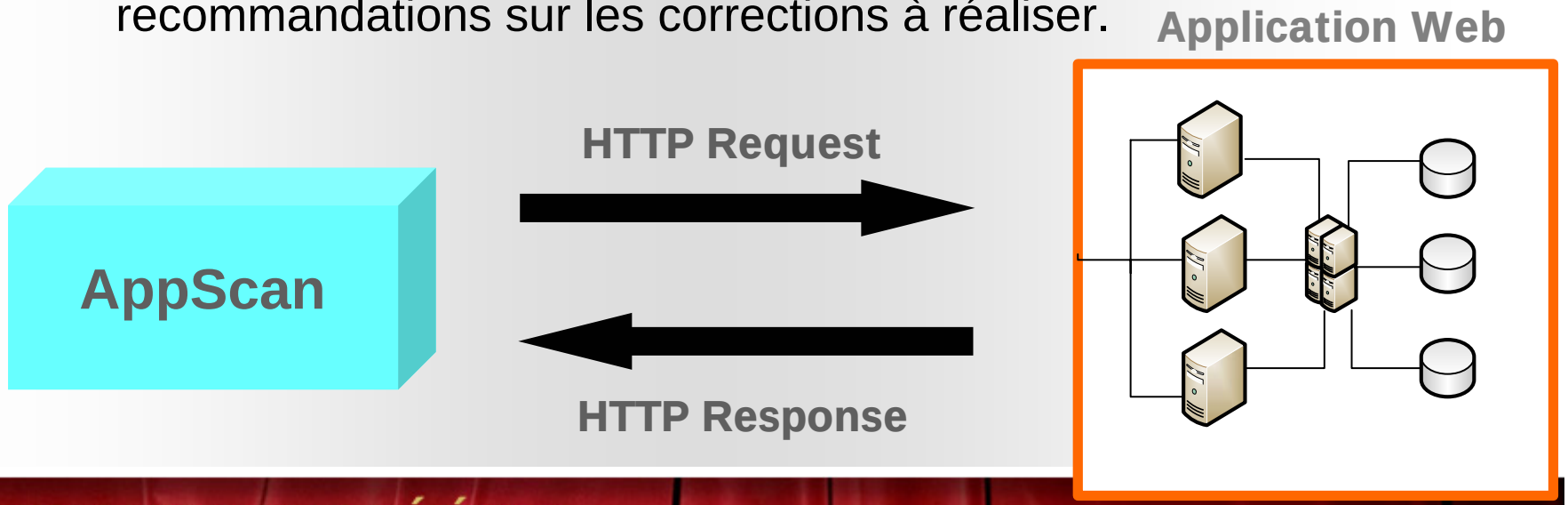
FIGURE 3 -INCIDENT BY ATTACK METHOD
("A" LABELS REFER TO THE OWASP TOP 10 POSITION)

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.

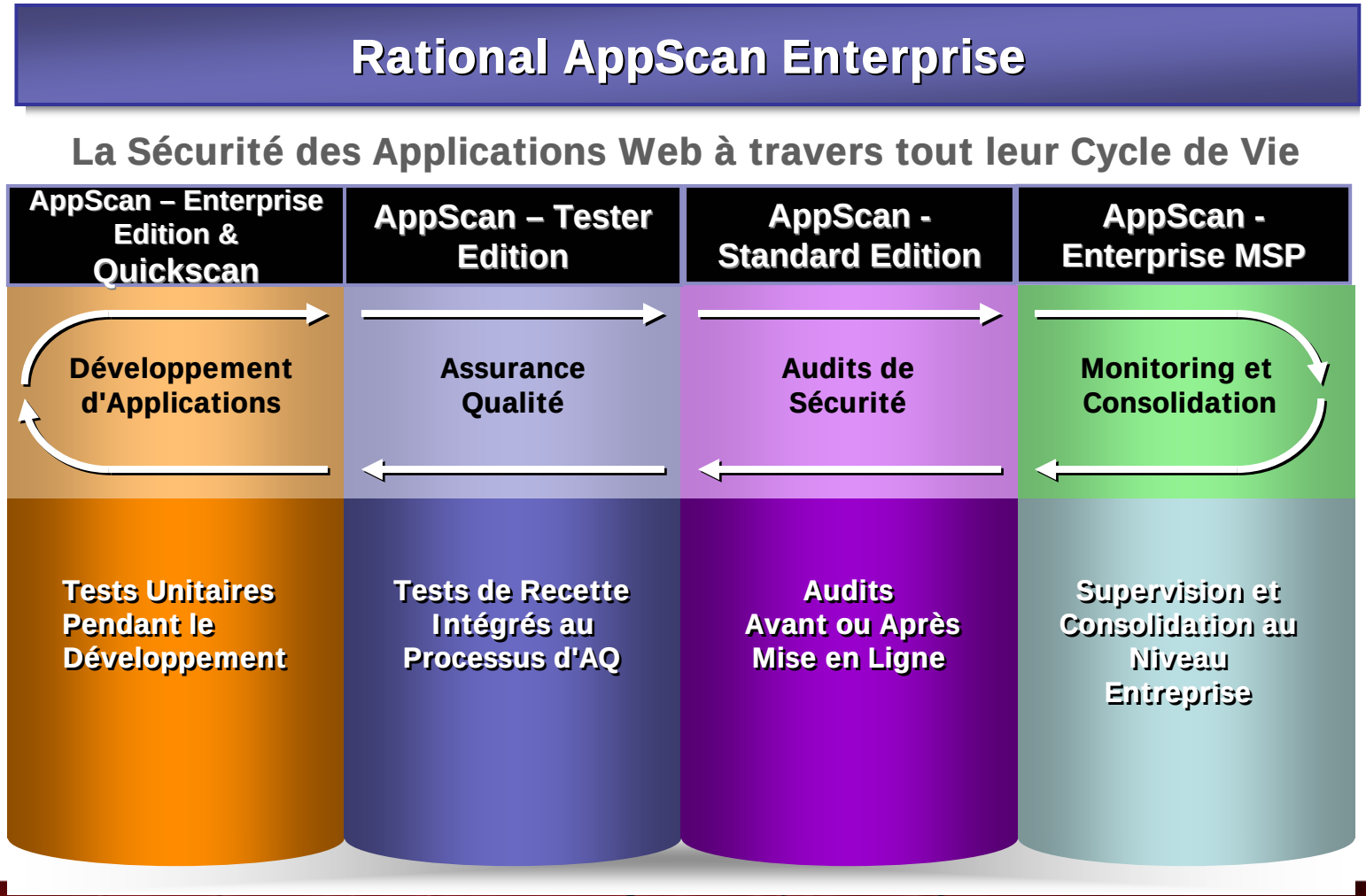
AppScan: Principe de fonctionnement

- 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.




DEMO

Famille des produits Rational AppScan



AppScan Enterprise

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

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