Audit des Applications & Services Web

avec

AppScan®

Présentation, Démonstration, Positionnement

Qui sommes nous?

- *AXIA+*
  - Société spécialisée dans le contrôle qualité et sécurité du contenu en ligne
  - Représentant de l'offre Watchfire pour la France
- **Watchfire**
  - Editeur canadien d'outils de test pour le web, depuis 1996
  - 200 personnes
    - Siège commercial à Boston
    - 2 centres de R&D (Canada et Israël).
- **AppScan**
  - Suite d'outils de tests & audits de la sécurité des applications et services web
  - #1 du marché des scanners de vulnérabilités applicatives

(*) selon les études 2006/2007 de Gartner Group et IDC

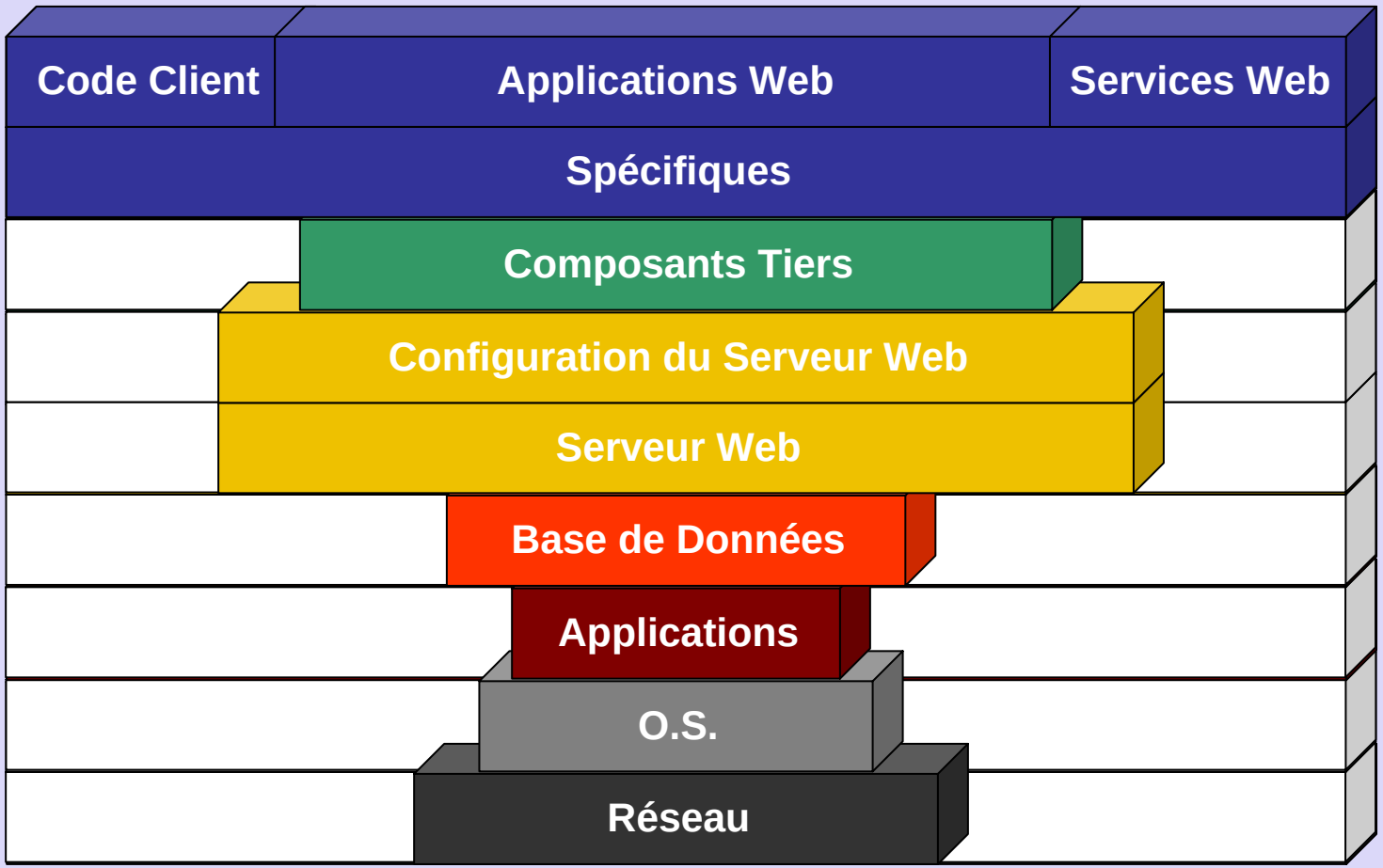
Où sommes nous?

Où sont les Vulnérabilités?

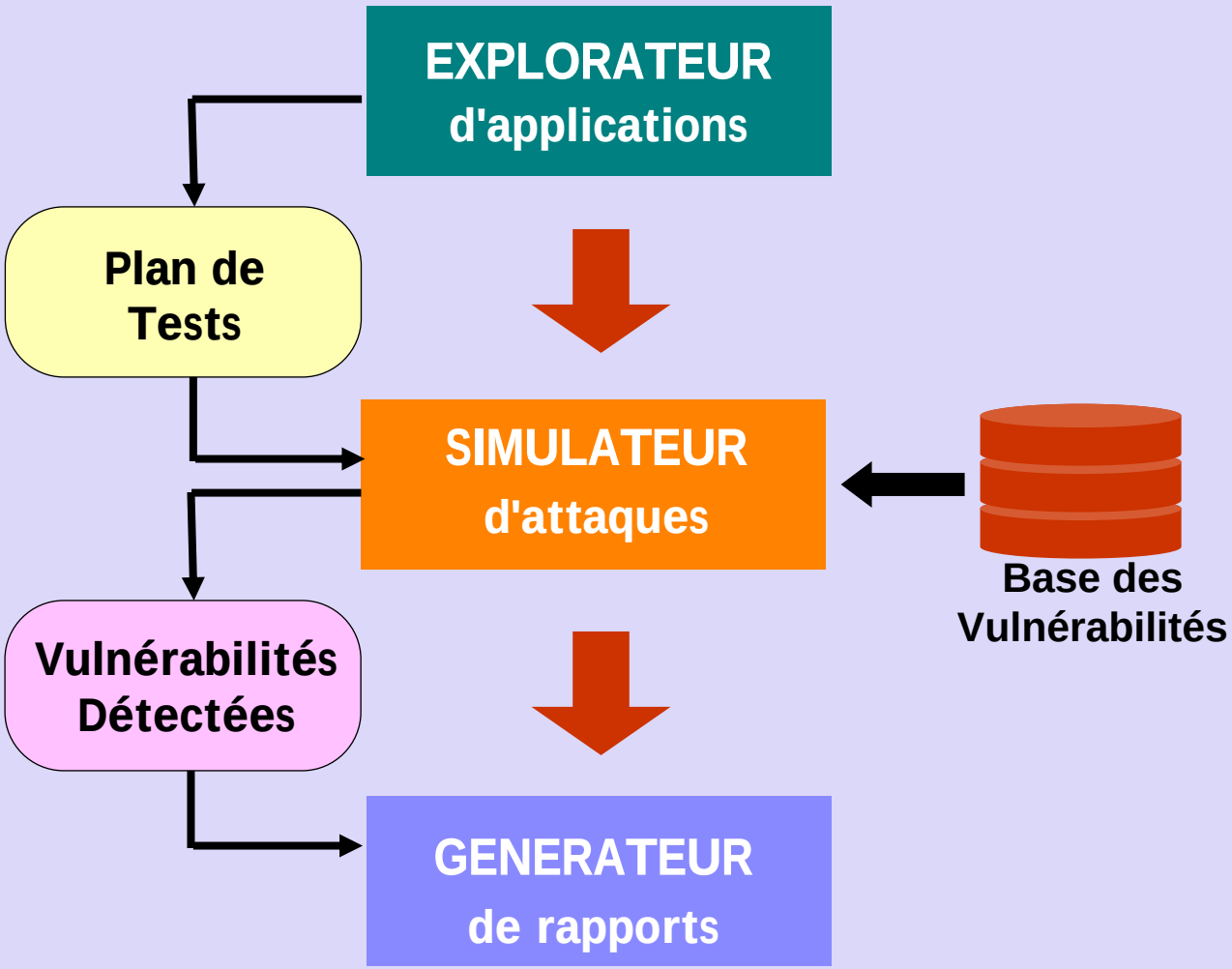
SCANNERS

Code Source (émergeant)

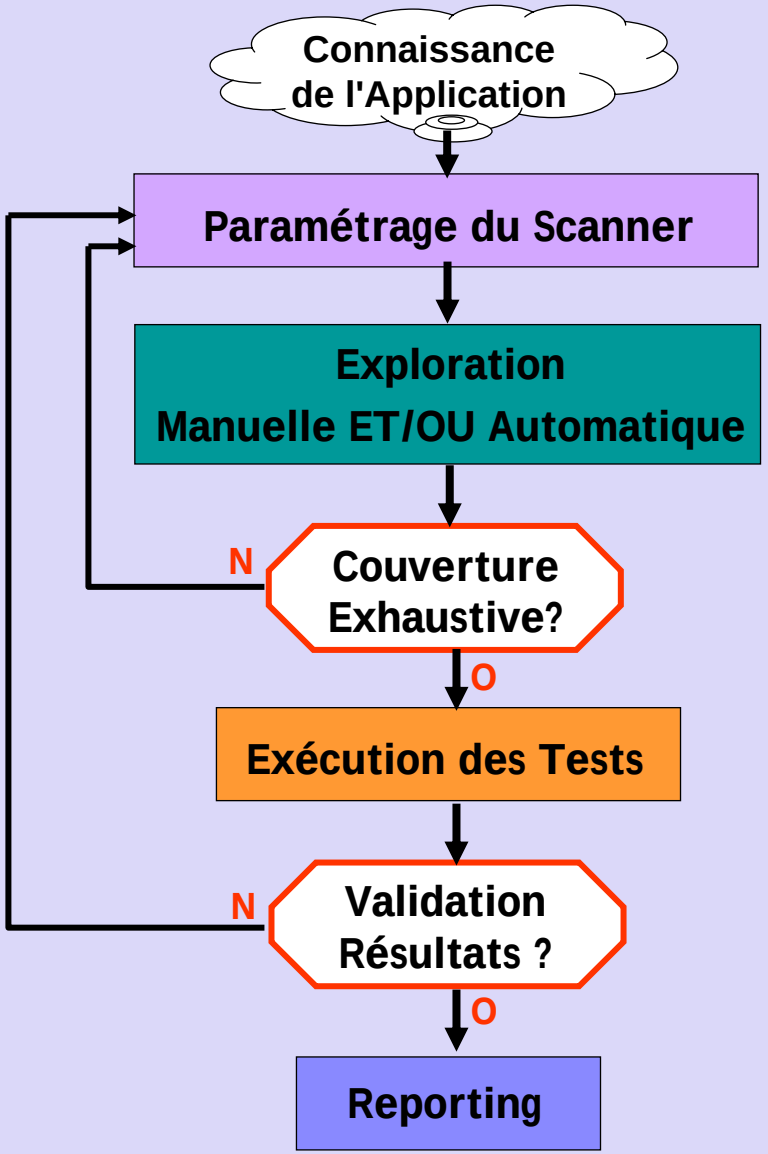
Fortify
Ounce Labs
Secure Software
Klockwork
Parasoft



AppScan: Principe de Fonctionnement



Le Processus d'Audit avec AppScan



Il est indispensable de connaître certaines caractéristiques de l'application

Quelle est la cible à scanner, comment la scanner, quels tests appliquer

Manuelle: enregistrement d'une session manuelle via le browser

Automatique: découverte des pages par le "crawler" de liens

Toutes les pages de la cible ont été visitées?

Tâche totalement automatique

Les vulnérabilités détectées sont-elles réelles?

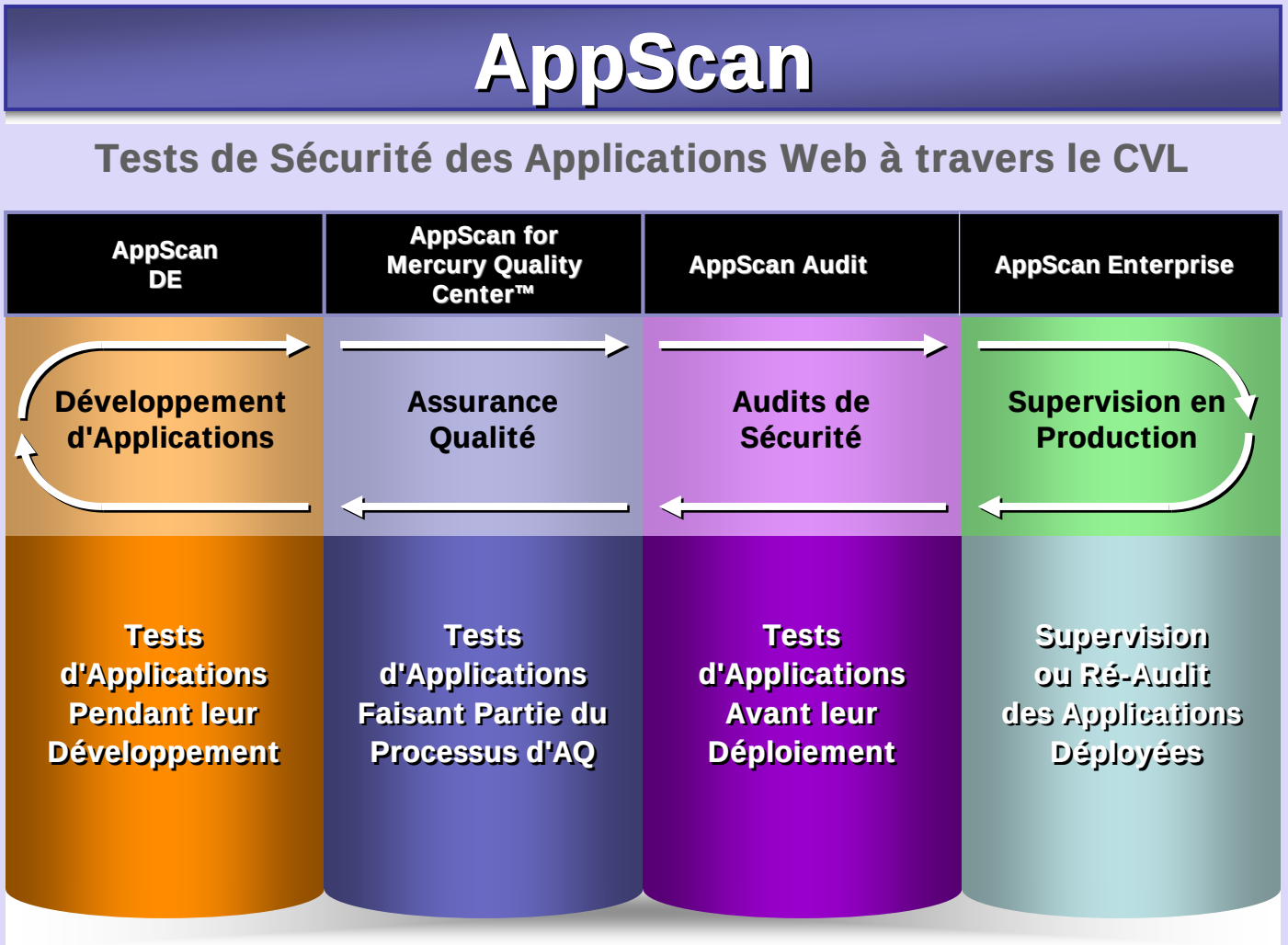
Génération de différents rapports de sécurité et de conformité réglementaire

Démonstration

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 tas de fonctions, mécanismes et outils complémentaires qui facilitent l'adoption de l'outil et son usage au quotidien

La Sécurité Applicative sur tout le Cycle de Vie du Logiciel



Merci de votre attention

Universalité & Puissance du Scanner

- Support de toutes les technologies actuelles, en matière de:
  - Applications web: JavaScript, Ajax, Flash, SSL…
  - Services web: WSDL, SOAP 1.1 et 1.2
  - Mécanismes d'authentification: HTTP, Formulaires HTML, NTML, certificats client
  - Systèmes anti-automates: CAPTCHA, 2FA…
  - Gestion de session: identifiants temporaires, variables/requête ou fixés par le client
  - Proxys: adressage et authentification
- Maintien automatique des sessions
  - Tests réguliers de l'état de la session et reconnexion automatique en cas d'expiration
  - Reconnaissance et gestion automatique des jetons de session les plus répandus
  - Paramétrage du mode de rafraîchissement des jetons spécifiques à une application
  - Détection automatique des pages de logout (paramétrable)
- Gestion complète des données de saisie obligatoires:
  - Saisie à priori (pendant le paramétrage)
  - Saisie par exploration manuelle (browser) et importation des valeurs
  - Détection des pages non explorées par manque de données obligatoires
  - Saisie interactive – à posteriori – de ces pages incomplètes
- Délimitation exacte de la cible par expressions régulières (inclusion/exclusion)
- Scanning "Multi-phases" : re-test automatique des pages révélées lors des tests

Etendue des Tests et Elaboration de Stratégies

- Une base de tests très riche
  - Tests applicatifs (universels): couvrent toutes les techniques d'attaque connues à ce jour, y compris les plus récentes (Port listening, HTTP response splitting etc.)
  - Tests d'infrastructure: + de 2000 vulnérabilités répertoriées, sur des centaines de produits commerciaux et open source, mises à jour quotidiennement
  - Tests d'élévation des privilèges: automatisation d'un type de test des plus fastidieux
  - Tests de Services Web
    - Outil simulant des appels aux services à partir des fichiers WSDL
    - Générateur de formulaires de saisie élaborés (tableaux, types énumérés etc.)
    - Stratégie des test prédéfinie pour les Services Web
  - Tests spécifiques/personnalisés
    - Tests d'ajout/modification de paramètres
    - Tests de recherche de pattern particulier dans une réponse serveur
    - Tests d'accès à des URLs particulières (infrastructure)
- Gestionnaire graphique des stratégies de test
  - Modèles réutilisables de stratégies, prédéfinis ou personnalisés
  - Description complète de chaque type de vulnérabilité
    - Description WASC, référence CVE, élément actif pour chaque variante de test
  - Contrôle total du choix des tests à appliquer
    - Regroupements par sévérité, type, niveau d'intrusion etc.
    - Recherches dans la base par mots-clés

Exploitation et Validation des Résultats

- Exploration et granularité
  - Listage des vulnérabilités pour chaque niveau de l'arborescence applicative
  - Visualisation (requête+réponse) de toutes les variantes d'un test pour chaque URL
- Lisibilité et compréhension
  - Mise en évidence des différences entre l'échange initial et celui du test: éléments modifiés par AppScan dans la requête et "témoins" présents dans la réponse
  - "Reasoning": explication du raisonnement amenant AppScan à conclure à la présence d'un vulnérabilité
  - "Advisory": description de la vulnérabilité selon le WASC, liens bibliographiques
  - Possibilité de capturer des copies d'écran (si résultat visuel) et les rajouter avec des commentaires dans les rapports
- Contrôle et validation des résultats
  - Facilités de contrôle l'exhaustivité de la couverture de l'application (Application Data)
  - Faux positifs: AppScan est l'outil avec le plus petit taux de faux positifs - (*Caleb Sima*)
    - Mécanisme automatique de remontée des faux positifs (vrais ou présumés) au support
  - Trace (personnalisable) de l'activité du scanner en temps réel
- Facilités et consignes de correction
  - Regroupement des tâches correctives par type: facilité de répartition entre intéressés
  - Conseils de correction, avec exemples de code en Java/J2EE ou .NET
  - Facilité de contrôle/suivi des corrections grâce aux rapports différentiels

Rapports de Sécurité et de Conformité

- Tous les rapports peuvent être générés à volonté, sans avoir à relancer le scan
- Personnalisation des rapports de sécurité, selon le destinataire: RSSI, Auditeur, Développeur, QA etc.
  - Choix du type et du niveau des détails à inclure, du type de test ou de la sévérité minimale à prendre en compte
  - Choix de certains éléments de présentation: titre, logos, descriptif, entête de page…
- Exportation des résultats du scan pour analyse avec des outils tiers:
  - Fichier au format XML
  - Base SQL (Firebird) avec pilote ODBC
- Très large couverture en termes de conformité réglementaire
  - >30 réglementations (inter)nationales ou standards de l'industrie supportés: PCI, SOX, ISO, OWASP, SANS…
  - Capacité de définir un standard de sécurité (policy) propre à l'entreprise
    - Définition en XML de règles de sécurité génériques, associées à différents types de vulnérabilités

Exploitabilité Accrue

- Exploration manuelle ET/OU automatique:
  - Exploration manuelle seule: tests de processus métier plus ou moins complexes
  - Exploration manuelle + automatique: résout le problème des authentifications complexes
  - Exploration totalement automatique: pour les sites relativement simples
- Possibilité d'interrompre et reprendre l'exécution du test: pratique sur des gros sites*
- Planification du lancement différé d'un scan (unique ou périodique)
- Téléchargement et mise à jour automatiques de la base des tests
- **PowerTools**: la panoplie du parfait "testeur de pénétration" pour compléter un audit automatisé et faciliter certaines opérations (livrés avec AppScan)
  - **Authentication Tester**: générateur de username/password pour attaques en force brute
  - **Token Analyzer**: analyseur statistique de SIDs évaluant leur prédictibilité
  - **Connection Test**: tests de ping en protocole HTTP
  - **HTTP Request Editor**: éditeur de requêtes HTTP
  - **HTTP Proxy**: proxy permettant de capturer et analyser des requêtes HTTP
  - **Encode/Decode**: utilitaire de codage/décodage selon différents formats et algorithmes
  - **Expression Test**: aide à la mise au point d'expression régulières

(*) Sachant que les résultats s'affichent au fur et à mesure que le scan progresse et qu'on peut les manipuler sans attendre la fin