IBM Software Group

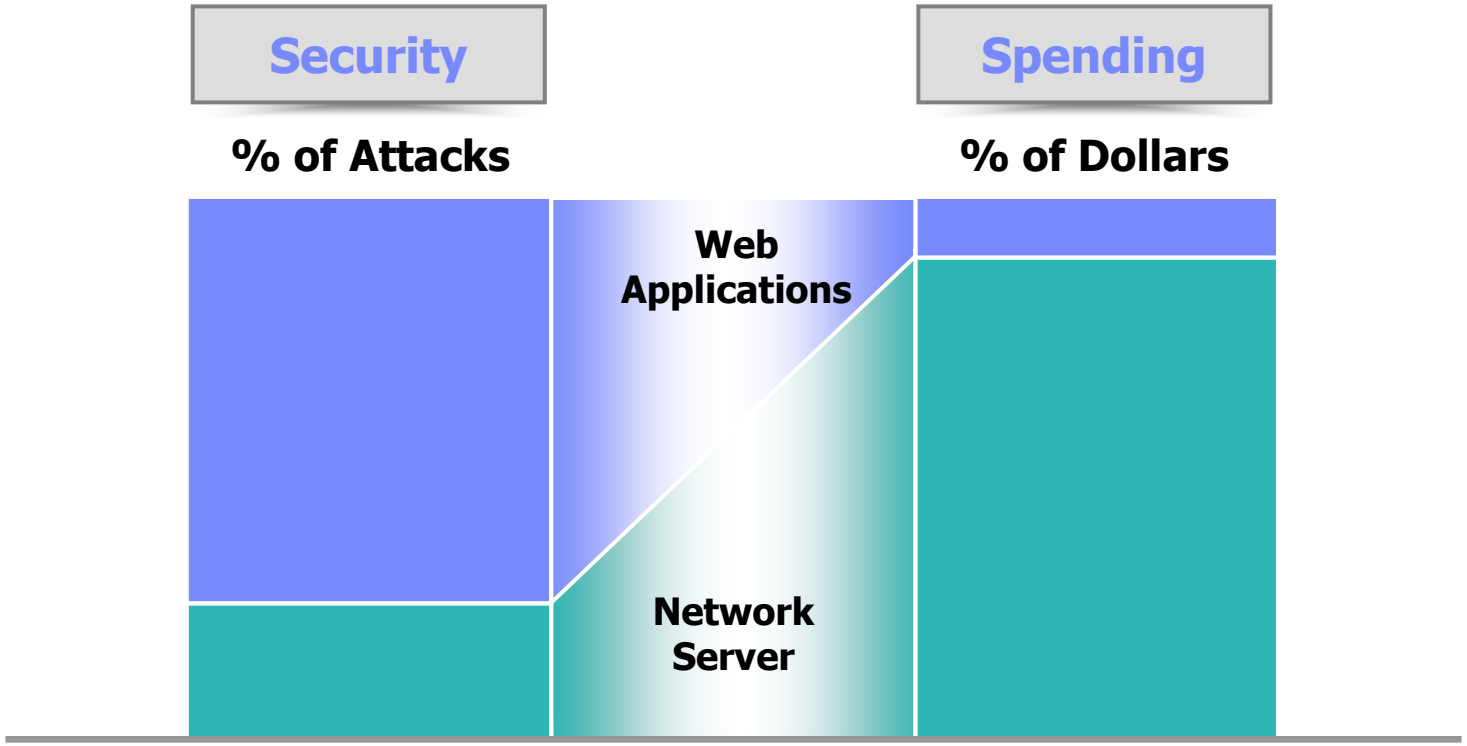
IBM Rational AppScan

Preisinger Balázs
Rational termékmenedzser

balazs.preisinger@hu.ibm.com
+36 20 823-5698

© 2009 IBM Corporation

A valóság



75% of all attacks on Information Security are directed to the Web Application Layer

2/3 of all Web Applications are vulnerable

Gartner

Sources: Gartner, Watchfire

Minőségbiztosítás kiterjesztése, bemutatkozik az IBM Rational AppScan és IBM Rational Policy Tester

IBM Rational AppScan	IBM Rational Policy Tester
Automatizált biztonsági tesztelő webes alkalmazásokhoz és webes szolgáltatásokhoz ✓ Méretezhető megoldás a biztonsági sebezhetőségek felderítésére és kiküszöbölésére. ✓Fejlesztőknek, tesztelőknek, biztonsági szakembereknek és vezetőknek készült. ✓ Jelentések készítése, nyomon-követhetőség	Minőség és megfelelőség tesztelő platform a webhely minőségének, titkosságának és megfelelőségének vizsgálatára és kezelésére ✓Quality Edition biztosítja a webhely funkcionalitását és a felhasználói elégedettséget ✓ Privacy Edition vizsgálja a megfelelőséget a különböző szigorú szabályozásoknak, mint pl.: ISO, HIPPA, COPPA, Safe Harbor ✓ Accessibility Edition biztosítja a webhely elérhetőségét és megfelelőségét

Web-alkalmazásokat fenyegető veszélyek

Támadás	Negatív hatás	Lehetséges üzleti kockázat
Buffer overflow	Denial of Service (DoS)	Oldal elérhetetlensége
Cookie poisoning	Session eltérítés	Lopás
Hidden fields	Oldal átalakítás	Illegális tranzakciók
Debug options	Admin hozzáférés	Jogosulatlan hozzáférés, személyes adatok védelmének sérülése
Cross Site scripting	Azonosító lopás	Lopás, ügyfél bizalmatlanság
Stealth Commanding	Hozzáférés OS-hez, alkalmazásokhoz	Hozzáférés személyes adatokhoz, csalás, stb.
Parameter Tampering	Csalás, adatlopás	Ügyfelek átirányítása
Forceful Browsing/ SQL Injection	Jogosulatlan oldal/adat hozzáférés	Írás/olvasás az ügyfél adatbázba/adatbázisból

Az IBM Rational Web Application Security előnyei

Company

- Több mint 10 éves tapasztalat a webes alkalmazások biztonsága, minősége és megfelelősége terén
- Szorosan együttműködő biztonsági és fejlesztői csapat
- Mi rendelkezünk a legtöbb felhasználóval -> legtöbb tapasztalat
- Piacvezető pozíció a Gartner & IDC szerint

Technology

- Legátfogóbb alkalmazás lefedettség – AJAX, Flash, Flex, stb.
- Megtalálja a legkomolyabb hibákat – WASC, OWASP, stb.
- Legkevesebb téves riasztás az iparban
- Megkönnyíti a kommunikációt a nem-biztonsági szakemberekkel
- Web-alapú megoldás a teljes vállalati bevezetéshez
- Számítógép-alapú oktatás és szolgáltatás -> legjobb-gyakorlat alapú hibajavítás

Webes alkalmazás tesztelés fejlődési modellje

Vállalati skálázhatóság
AppScan Enterprise

- Skálázhatóság és teljes lefedettség a fejlesztés bevonásával a tesztelésbe

Vállalati láthatóság
AppScan Reporting Console

- Konszolidáció a fejlesztés és menedzsment jelentéseinek láthatóságáért és elosztásáért

Belső auditok
AppScan Desktop

- Belső tesztelés, a biztonsági audit csapat által vezetett alkalmazás ellenőrzésekkel

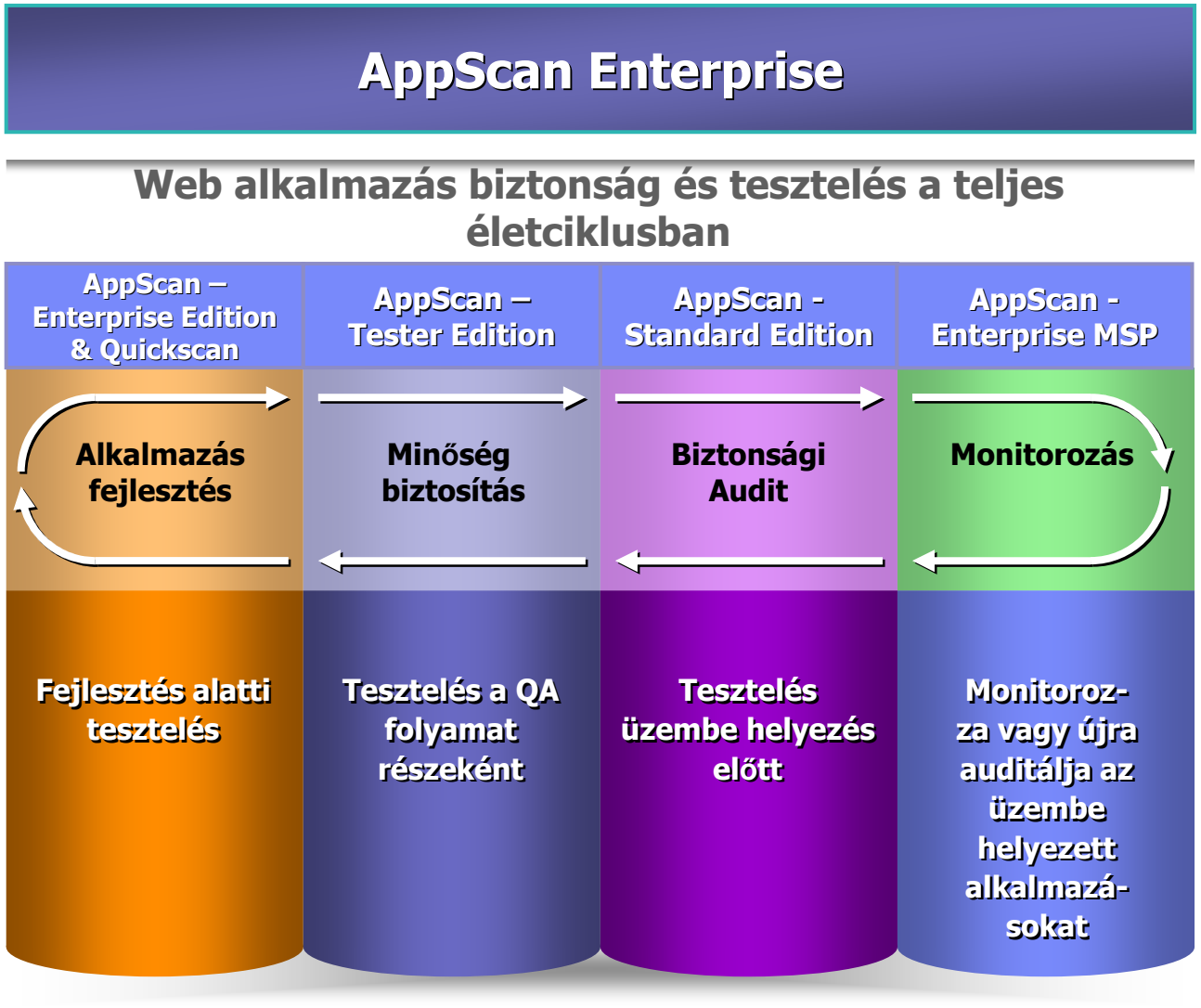
Külső auditok
AppScan OnDemand

- Elkezdik tesztelni az alkalmazások sebezhetőségét

Az IBM Rational AppScan család

Express Edition	Biztonsági megoldás kis- és közepes vállalkozások számára
Standard Edition	Általános asztali megoldás az automatizált biztonsági teszteléshez
Tester Edition	QA folyamatba integrált biztonsági megoldás
Developer Edition	Biztonsági megoldás a fejlesztőknek, ahol még a legolcsóbb a hibák javítása
Build Edition	Beépíti a biztonsági tesztelést a build menedzsment folyamatba
Reporting Console	Központosított adatgyűjtés és riportolás
Enterprise Edition	Web-alapú, többfelhasználós, központosított megoldás párhuzamos teszteléshez és riportoláshoz

Webes alkalmazás biztonsági tesztelő eszközök




DEMO

KÉRDÉSEK
&
VÁLASZOK