Challenges and Solutions

Amit Ashbel
Product Marketing Manager
Amit.ashbel@checkmarx.com
June 2015
About Checkmarx

- Founded in 2006
- Enterprise Grade Application Security Solutions:
  - SAST  |  RASP  |  Application Security Education
- Hundreds of Fortune 500 and SMB Customers
- ~150 Employees WW
- Fanatical support

Awards

- "Leader" in the 2014 AST Wave
- "Challenger" - 2014 AST Magic Quadrant & Only Vendor to score a perfect 5 in 2014 AST Critical Capabilities Report
- Fastest Growing Security Company in Israel, 2014 Tech Fast 500
- Red Herring EMEA Top 100 Winners
High Profile breaches

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Challenges
Challenge #1: Lack of secure coding knowledge
Solution #1 Education & Awareness

- Application security education and awareness is needed throughout the entire development and deployment organization

- What are the impacts of unsecure code
- Measure your developers by quality and security
- Buy-in your developers
- Make sure developers have something to gain
- Make the process transparent for developers
Solution #1: Scan & Fix - see where and how to fix the vulnerability

What to fix

How to Fix

Who should Fix

Where to Fix
Challenge #2: Outnumbered
Solution 2#: Automate the process

Developers
- Visual Studio
- TeamMentor

Source repository
- git
- SVN
- PERFORCE
- Visual Studio TFS

Fix suggestions
- TeamMentor

Build management
- Bamboo
- Jenkins
- Web Service API
- TeamCity
- CLI
- Visual Studio TFS

Bug tracking
- JIRA

Auditor control panel
- CxAudit
- Checkmarx web client

Integrations
- Dashboards
- sonar
- ThreadFix
- DAST
- NTObjectives

Enforce your security policy in the SDLC
Challenge #3: Lack of budget
Solution 3#: SAST reduces # of security bugs

# Bugs/ year

- PenTesting DAST
- Centralized SAST
- SAST as part of the SDLC

Timeline:
- Today
- +6 months
- +12 months
Most vulnerabilities are created during coding.

- 85% of bugs are found during coding.

Cost of repairing at each phase:
- $25 at coding
- $100 at unit tests
- $250 at function test
- $16000 at post release

Defects introduced at each phase:
- $25 at coding
- $100 at unit tests
- $250 at function test
- $1000 at post release

Resolve your vulnerabilities here.
Thank You!

Amit Ashbel
amit.ashbel@checkmarx.com