How Do You Eliminate the IT Security Bottleneck?

How to get the most out of your tools

Presenter: Will Bechtel

SANS AppSec 2012
Will Bechtel – Director of Product Management, Qualys
  Web Application Scanning (WAS)
  Malware Detection Service (MDS)

Previous Experience
  Application Security Practice Lead – AT&T Consulting
  Sr. Consulting Manager VeriSign Global Security Consulting
  Application/Product Development (13+ years)

If Certifications matter…
  CISSP, CISA, PMP
Visible Targets

“The inherent need for many web applications to be Internet visible makes them a logical target”

Associated with Data Loss

“Web Applications….were associated with over a third of total data loss”

Popular and Successful Attack Vector

“Web applications abound in many larger companies, and remain a popular (54% of breaches) and successful (39% of records) attack vector. “
The costs for fixing security flaws are dramatically lower the earlier in the development lifecycle they are fixed.
S&P 500 Food Company
Over 10,000 employees, 5 billion in revenue

Developer
App Owner

IT Security
Scanner

Report of Scan Results

All vulnerability info comes from IT Security

Developer

Fix Code

Scan App

Dev App1

QA App1

UAT-App1

Prod-App1

Promote
Promote
Promote

Developers don’t know until later in LC that there are issues
Eliminating IT Security Bottleneck

All Stakeholders Participate

Scan Dev
Developer

Scan QA
QA

Reports
App Owner

Oversight /Production Scanning
IT Security

Fix Code
Cloud Portal

Vulnerabilities are identified and fixed early in lifecycle

Dev App1
Promote

QA App1
Promote

UAT-App1
Promote

Prod-App1