Developing a Software Security Assurance Program

Presented by Kabir Mulchandani

Managing Principal, Cigital

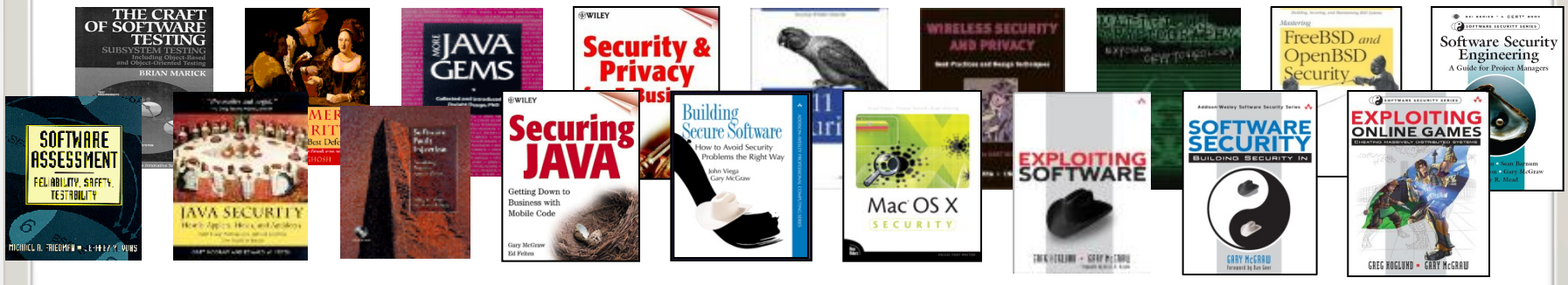
Agenda

- Introduction
- What is Software Security Assurance?
- Why is Software Security Assurance important?
- What does a Software Security Assurance Program look like?
- Elements of a Software Security Assurance Program
- Developing a Program
- Assessing Your Software Security Assurance Program
- Moving Forward
- Questions and Answers

Introduction

- Founded in 1992 to provide software security and software quality professional services
- Recognized experts in software security
  - Widely published in books, white papers, and articles
  - Industry thought leaders

cigital



What is Software Security Assurance?

- Ensuring software is designed and developed to minimize risks to an organization
- Risks may include data integrity, data leakage, data misuse, website defacement, etc.
- Capabilities across the organization to ensure software is built securely throughout the SDLC
- Software security assurance is an application of risk management techniques throughout the SDLC

What is Software Security Assurance?

Components

- Software Security Initiative (SSI)
  - An effort dedicated to improving the security of all deployed software
  - Includes responsibility for software security in vendor environments
- Software Security Group (SSG)
  - Team with the mandate to ensure software security
  - Responsible to define, implement and enforce software security policies and standards throughout the SDLC

Why is Software Security Assurance important?

Major Drivers Influencing SSA Programs

- Compliance
- Contractual
- Reactionary
- Security

Why is Software Security Assurance important?

Some Trends Influencing SSA Programs

- Traditional focus on network and perimeter, but attack surface is shifting to application software
- The proliferation of end-user applications has created more code, more insecure code, more vulnerabilities
- Emergence of "do-it-yourself" development toolkits and easy-to-learn programming languages have introduced more new developers with little or no security knowledge

Why is Software Security Assurance important?

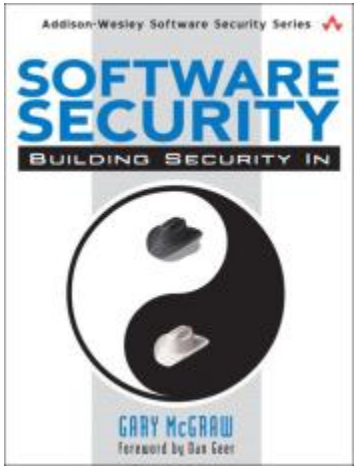
A Shifting Trend

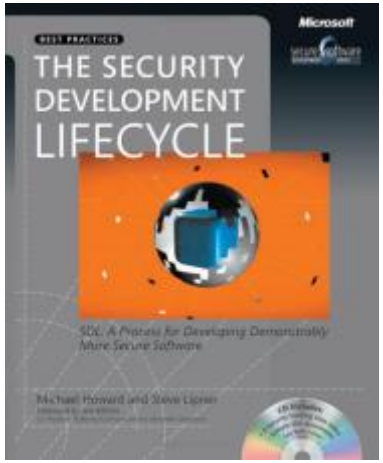
- Many software security programs focus on pre-deployment penetration testing, late in the SDLC
- Primary focus is on finding implementation bugs and bolting on security controls
- Organizations are now learning that software security needs to be integrated within the SDLC
- Preventive measures need to be established to avoid bugs and to define security architecture early in the SDLC to prevent flaws at inception

What does an SSA Program look like?

Integrating best practices into large organizations

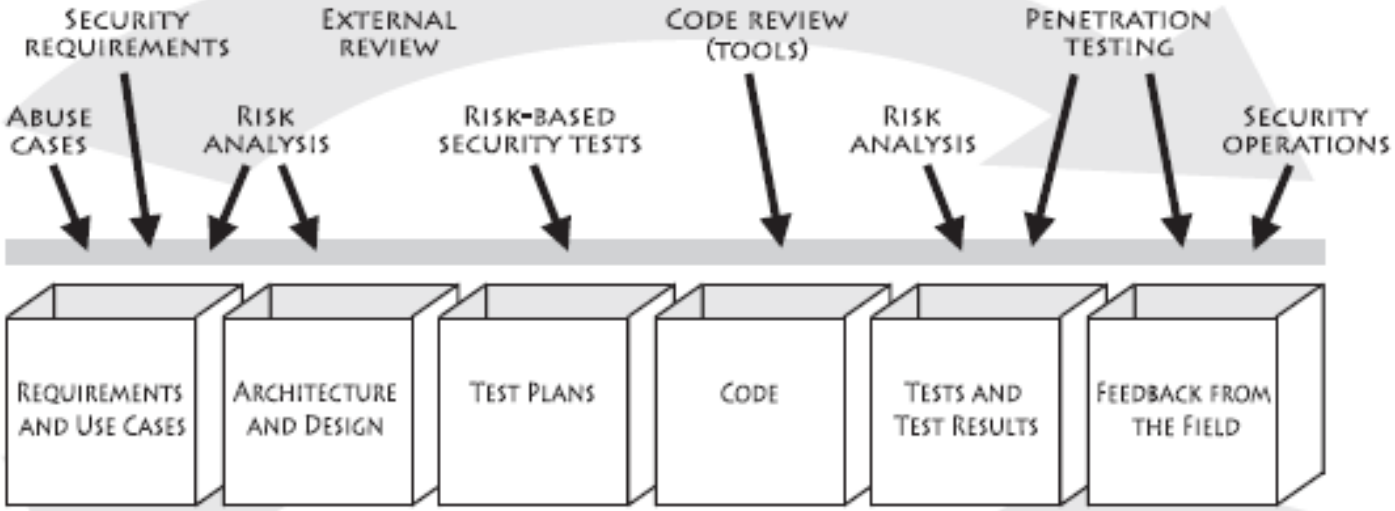
- Microsoft's SDL
- Cigital's Touchpoints
- OWASP Comprehensive, Lightweight Application Security Process (CLASP)





What does an SSA Program look like?

software security touchpoints



What does an SSA Program look like?

BSIMM: software security measurement

- Real data from (42) real SSA initiatives
- 81 measurements
- McGraw, Chess, & Migues

cigital

PlexLogic

FORTIFY

CSO

Minded security

VIRTUALFORGE
we harden your software

What does an SSA Program look like?

software security framework

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

- Four domains, twelve practices
- A 'blueprint' for a SSA Program based on best practices

Elements of an SSA Program

Governance

- ***Strategy and Metrics*** – Planning, assigning roles and responsibilities, identifying software security goals, determining budgets, identifying metrics and gates.
- ***Compliance and Policy***– Identifying controls for compliance regiments, developing contractual controls (COTS SLA), setting organizational policy and auditing against policy.
- ***Training***– Establishing awareness and training programs and campaigns, hosting internal and external software security events and promoting a culture of software security.

Elements of an SSA Program

Intelligence

- ***Attack Models***– Establishing threat modeling, abuse cases, data classification, and technology-specific attack patterns.
- ***Security Features and Design***– Identifying security patterns for major platforms, middleware frameworks and providing proactive security guidance early in the SDLC.
- ***Standards and Requirements***– Defining explicit security requirements, coding standards, managing use of open source technologies and establishing a standards review board.

Elements of an SSA Program

Secure Software Development Lifecycle Touchpoints

- ***Architecture Analysis***– Capturing software architecture diagrams, applying lists of risks and threats, adopting a process for review, and building an assessment and remediation plan.
- ***Code Review***– Use of code review tools (e.g., HP Fortify, IBM AppScan), development of customized rulesets, manual analysis and ranking/measuring results.
- ***Security Testing***– Use of black box testing, risk driven white box testing, application of the attack model and code coverage analysis.

Elements of an SSA Program

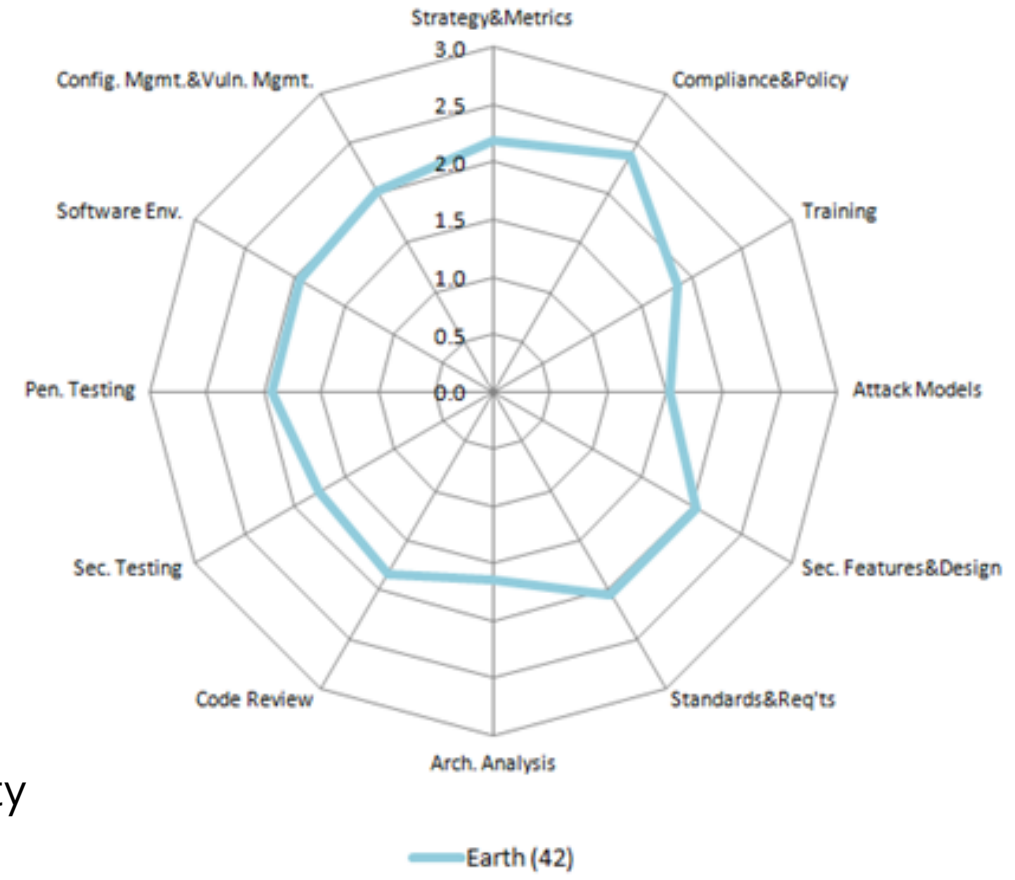
Deployment

- ***Penetration Testing***– Using automated and manual testing methods to assess vulnerabilities in final configuration and remediation based on residual risks.
- ***Software Environment***– Ensuring OS and platform patching, use of web application firewalls, install and config. documentation, application monitoring, change management and code signing.
- ***Config. Management and Vulnerability Management***– Ensuring procedures are in place for patching and updating applications, version control, defect tracking and remediation and incident handling.

Twelve things "almost everybody" does (66%)

Core activities

- Identify SDLC gates
- Know PII obligations
- Awareness training
- Data classification & inventory
- Build security features
- Security standards
- Review security features
- Static analysis tools
- QA boundary testing
- External pen testers
- Good host/network security
- Close ops bugs loop



Developing an SSA Program

Building a program from the ground up:

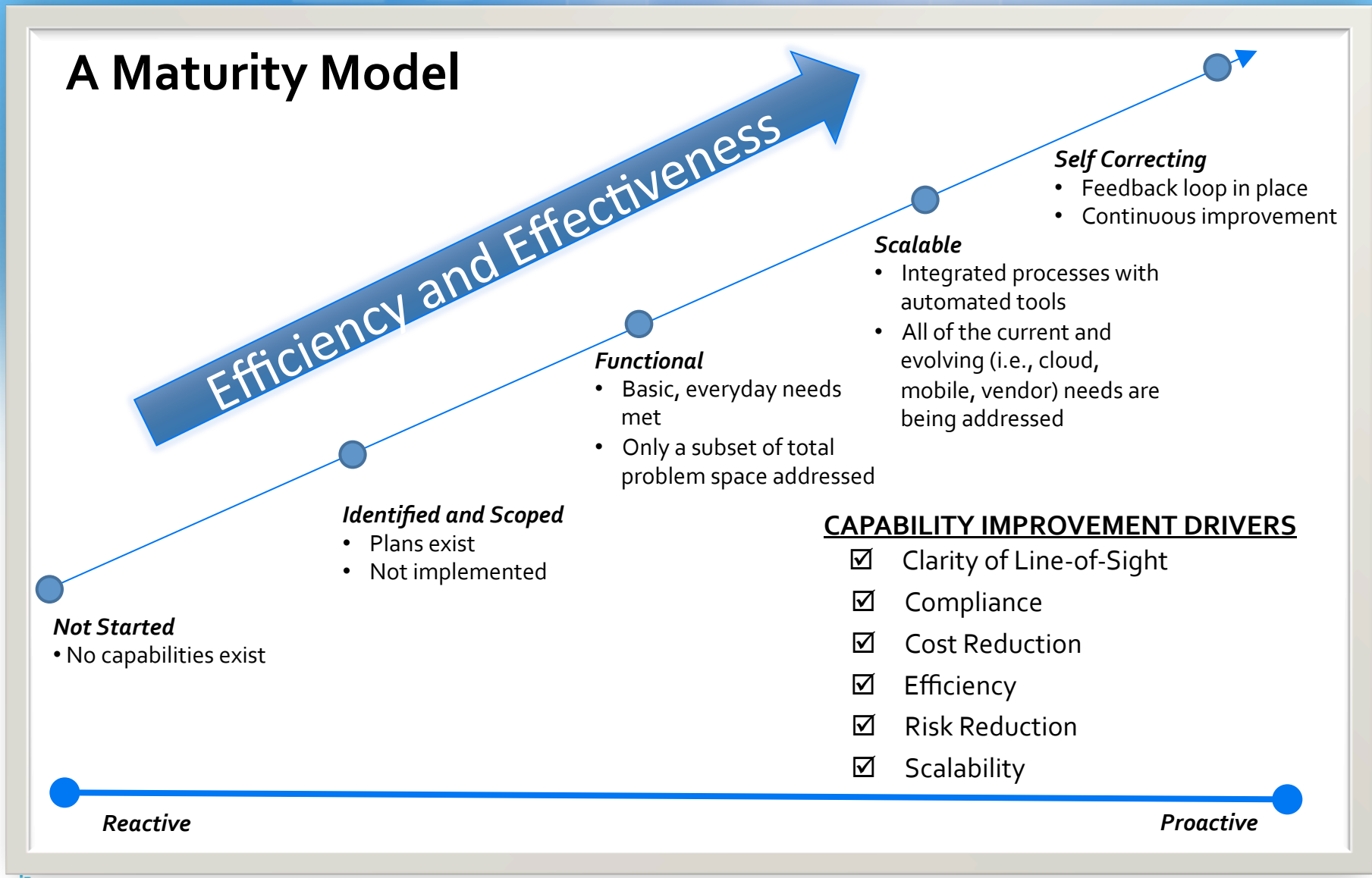
- Establish the Software Security
- Build the Software Security Group
- Develop strategy, policies and standards
- Integrate SDLC checkpoints
- Analyze the application portfolio
- Establish metrics
- Conduct training and awareness activities

Developing an SSA Program

Improving on already existing program:

- Expand scope
- Engage earlier
- Invest in competencies across the SDLC
- Automate
- Achieve scalability

Assessing and improving your SSA Program



Moving Forward

- Establish the objectives of your SSA program
- Conduct a risk assessment, ensure you address all emerging risk areas
- Assess the maturity of your program, if one exists
- Develop a plan to initiate or enhance the program
- Continue with training and awareness initiatives
- Execute your plan
- Establish a process to periodically re-evaluate your program and look for continuous improvement opportunities

Questions and Answers

Thank you for your attention