Do You Have a Scanner
Or Do You Have a Scanning Program?

Dan Cornell
@danielcornell
Denim Group Background

• Professional services firm that builds & secures enterprise applications
  – *External application assessments*
    • Web, mobile, and cloud
  – *Software development lifecycle development (SDLC) consulting*
• Classroom and e-Learning for PCI compliance
• Secure development services:
  – *Secure .NET and Java application development*
  – *Post-assessment remediation*
• Deep penetration in Energy, Financial Services, Banking, Insurance, Healthcare and Defense market sectors
• Customer base spans Fortune 500
• Contributes to industry best practices through the Open Web Application Security Project (OWASP)
Dan Cornell

- Dan Cornell, founder and CTO of Denim Group
- Software developer by background (Java, .NET, etc)
- OWASP San Antonio
- 15 years experience in software architecture, development and security
- Heads Denim Group’s application security team
Who Here Has Purchased an Automated Scanner?

- Static or Dynamic? (Or Both?)
- Desktop, Enterprise or Cloud (Or All the Above?)
Who Here Is Happy With Their Scanner?

- Yes
- No
- Kind Of
- Not Sure
Why or Why Not?
Successful Software Security Programs

• Common Goal
  – *Reduce Risk by*…
    • Reliably Creating Acceptably Secure Software

• Obligatory “People, Process, Technology” Reference
  – *Anybody got a good Sun Tzu quote?*
  – *I’d settle for a von Clausewitz*…
  – *Or perhaps we need to look at Dalai Lama quotes (topic for a different day)*

• Common Activities
  – *Implementation must be tied to the specific organization*
Software Assurance Maturity Model (OpenSAMM)

• Open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks racing the organization

• Useful for:
  – Evaluating an organization’s existing software security practices
  – Building a balanced software security program in well-defined iterations
  – Demonstrating concrete improvements to a security assurance program
  – Defining and measuring security-related activities within an organization

• Main website:
  – http://www.opensamm.org/
SAMM Business Functions

• Start with the core activities tied to any organization performing software development
• Named generically, but should resonate with any developer or manager

This slide content © Pravir Chandra
SAMM Security Practices

- From each of the Business Functions, three Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a ‘silo’ for improvement

This slide content © Pravir Chandra
# Check Out This One...

## Education & Guidance

**Objective**
- **EG 1**: Offer development staff access to resources around the topics of secure programming and deployment
- **EG 2**: Educate all personnel in the software life-cycle with role-specific guidance on secure development
- **EG 3**: Mandate comprehensive security training and certify personnel for baseline knowledge

## Activities

**A.** Conduct technical security awareness training
- **B.** Build and maintain technical guidelines

**A.** Conduct role-specific application security training
- **B.** Utilize security coaches to enhance project teams

**A.** Create formal application security support portal
- **B.** Establish role-based examination/certification

*This slide content © Pravir Chandra*
What Part Does Scanning Play?

- Automated scanning is part of both the “Security Testing” and “Code Review” Security Practices within the Verification Business Function
  - *Dynamic scanning and static scanning, respectively*

- Common starting point for many organizations embarking on software security programs
  - *There are lots of commercial and freely available products that can be used in support of this activity*

**RED FLAG:**

Q: What are you doing for software security?
A: We bought [Vendor Scanner XYZ]

*** BEWARE FOSTERING A CHECKBOX CULTURE ***
Scanning Program: Anti-Patterns

• “Dude With a Scanner” approach
  – Can also be implemented as the “lady with a scanner” approach

• “SaaS and Forget” approach
Is Your Scanner Missing Something?

- **Breadth “Misses”**
  - *Inadequate application portfolio*
  - *Applications not being scanned or not being scanned frequently enough*

- **Depth “Misses”**
  - *Ineffective crawling ignores application attack surface*
  - *False negatives resulting in ignorance of legitimate vulnerabilities*
  - *Excessive false positives causing results to be ignored*
Security Testing: Better Patterns

• **Breadth-First Scanning**
  – You want a scanning program, not a scanner

• **Deep Assessment of Critical Applications**
  – Automated scanning, manual scan review and assessment

• **Understand that scanning is a means to an end**
  – Not an end in and of itself
  – Start of vulnerability management
What Goes Into a Good Scanning Program?

- Solid Understanding of Attack Surface
- Realistic Concept of Scanner Effectiveness
- Disciplined History of Scanning
- Prioritized Testing Efforts
What Is Your Software Attack Surface?

Software You Currently Know About

What?
• Critical legacy systems
• Notable web applications

Why?
• Lots of value flows through it
• Auditors hassle you about it
• Formal SLAs with customers mention it
• Bad guys found it and caused an incident (oops)
What Is Your Software Attack Surface?

Add In the Rest of the Web Applications You Actually Develop and Maintain

What?
- Line of business applications
- Event-specific applications

Why Did You Miss Them?
- Forgot it was there
- Line of business procured through non-standard channels
- Picked it up through a merger / acquisition

What?
What Is Your Software Attack Surface?

**What?**
- More line of business applications
- Support applications
- Infrastructure applications

**Why Did You Miss Them?**
- Most scanner only really work on web applications so no vendors pester you about your non-web applications
- Assume the application vendor is handling security

Add In the Software You Bought from Somewhere
What Is Your Software Attack Surface?

What?
- Support for line of business functions
- Marketing and promotion

Why Did You Miss Them?
- Any jerk with a credit card and the ability to submit an expense report is now runs their own private procurement office
Attack Surface: The Security Officer’s Journey

- Two Dimensions:
  - Perception of Software Attack Surface
  - Insight into Exposed Assets
As perception of the problem of attack surface widens, the scope of the problem increases.
Attack Surface: The Security Officer’s Journey

- As perception of the problem of attack surface widens the scope of the problem increases
Attack Surface: The Security Officer’s Journey

- As perception of the problem of attack surface widens the scope of the problem increases
As perception of the problem of attack surface widens, the scope of the problem increases.
As perception of the problem of attack surface widens the scope of the problem increases.

**Attack Surface: The Security Officer’s Journey**

- Web Applications
- Client-Server Applications
- Desktop Applications
- Cloud Applications and Services
- Mobile Applications

Perception vs. Insight
Attack Surface: The Security Officer’s Journey

- Discovery activities increase insight
Attack Surface: The Security Officer’s Journey

- Discovery activities increase insight
Attack Surface: The Security Officer’s Journey

• Discovery activities increase insight
Attack Surface: The Security Officer’s Journey

- Over time you end up with a progression
Attack Surface: The Security Officer’s Journey

- Over time you end up with a progression
Attack Surface: The Security Officer’s Journey

- Over time you end up with a progression
Attack Surface: The Security Officer’s Journey

- Over time you end up with a progression
Attack Surface: The Security Officer’s Journey

- Over time you end up with a progression
Attack Surface: The Security Officer’s Journey

- When you reach this point it is called “enlightenment”
- You won’t reach this point
What Goes Into An Application Test?

An Application Test
What Goes Into An Application Test?

Dynamic Analysis

Static Analysis
What Goes Into An Application Test?

- Automated Application Scanning
- Static Analysis
- Manual Application Testing
What Goes Into An Application Test?

- Automated Application Scanning
- Automated Static Analysis
- Manual Application Testing
- Manual Static Analysis
# What Goes Into An Application Test?

<table>
<thead>
<tr>
<th>Unauthenticated Automated Scan</th>
<th>Authenticated Automated Scan</th>
<th>Automated Static Analysis</th>
</tr>
</thead>
</table>
What Goes Into An Application Test?

- Unauthenticated Automated Scan
- Authenticated Automated Scan
- Automated Source Code Scanning
- Automated Binary Analysis
- Blind Penetration Testing
- Informed Manual Testing
- Manual Source Code Review
- Manual Binary Analysis
Value and Risk Are Not Equally Distributed

• Some Applications Matter More Than Others
  – Value and character of data being managed
  – Value of the transactions being processed
  – Cost of downtime and breaches

• Therefore All Applications Should Not Be Treated the Same
  – Allocate different levels of resources to assurance
  – Select different assurance activities
  – Also must often address compliance and regulatory requirements
Do Not Treat All Applications the Same

- Allocate Different Levels of Resources to Assurance
- Select Different Assurance Activities
- Also Must Often Address Compliance and Regulatory Requirements
ThreadFix Demonstration

• Building Your Application Portfolio

• Storing Scanning Results Over Time

• Reporting
  – Trending
  – Vulnerability Remediation Progress
  – Scanner Benchmarking
  – Portfolio Status
Steps for Improvement

• Build Your Application Portfolio

• Characterize the Effectiveness of Efforts Made to Date

• Build a Plan for Coverage

• Monitor Progress
Questions / Contact Information

Dan Cornell
Principal and CTO
dan@denimgroup.com
Twitter @danielcornell
(210) 572-4400

www.denimgroup.com
blog.denimgroup.com