



# Enterprise Application Security Practices: Real-world Tips and Techniques

Mike Crague  
Dell Inc.

**OWASP**

June 24, 2010

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**

<http://www.owasp.org>

# Agenda

## Section One: Program Overview

- Dell's Information Security Organization
- Policies / Standards for Secure Application Development
- Awareness/Education/Training
- Addressing Global Standardization Issues
- Deploying an SDL as an Overlay to the SDLC
- Partnerships with Privacy, Legal, Compliance

## Section Two: Consultant Team

- Security Consulting Staff Development
- Division of Labor for Security Consultants
- Risk Assessments
- Security Reviews
- Threat Modeling
- Source Code Scans
- Pre-deployment Scans
- Penetration Testing
- Q&A



# Section One

# Program Overview

# Our Information Security Organization

## Global Information Security Services

Identity  
Management

eForensics

Security  
Consulting

Engineering

Incident  
Response &  
Assurance

Security Consulting is the outward-facing information security team; our mission is to manage and reduce security risks for our Dell Business Unit customers (IT, Services, Product Group, etc.)



# Policies/Standards for App Dev

- **Should be tied to root policy**
- **Complete standard re-write; tool-agnostic**
- **Socialization with developers, testers, compliance team, and VPs**
- **Approval at CIO staff was easy to get**
- **Revisions at procedure-level after 2 years**
- **Exception management and escalation process**

**Overcoming concerns of developers, business partners, compliance, and IT execs requires front-line success stories and realistic goals.**

# Awareness, Education, and Training

- **Outside speakers (Michael Howard from MS)**
- **Employee orientation**
- **Annual privacy/security course for all employees**
- **One-time first course for developers**
- **30-minute crash courses on 10 topics via CBT**
- **Security Consulting portal**
- **Security User Groups**
- **Communities of Practice**

**Having a marketing/communications specialist  
on the team helps immensely**

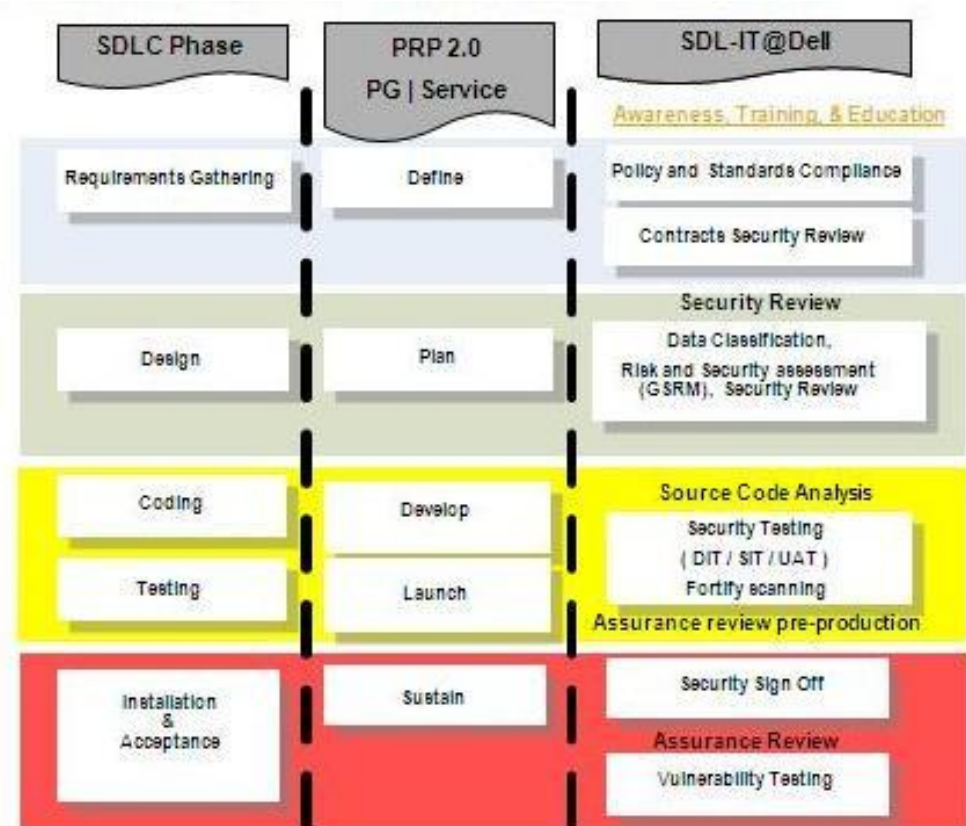
# Addressing Global Standardization Issues

- Enterprise Architecture standards review board
- Java and .NET
- Eclipse Ganymede, Galileo
- VS 2003 / 05 / 08
- XP, Vista, Windows 7
- MS Team Foundation Server for source control
- ASP 3.0, C, C++, Python, Perl, PHP, VB, Cold Fusion, COBOL
- Red Hat, SUSE, Oracle Enterprise Linux
- Novell
- VMWare
- Acquisitions and divestitures

**Lack of a standardized developer desktop has been one of our greatest challenges**

# SDL Checkpoints in the SDLC

- Getting embedded early, with simple checkpoints
- IT / Services / Product Group tailoring
- Traditional versus Agile methods



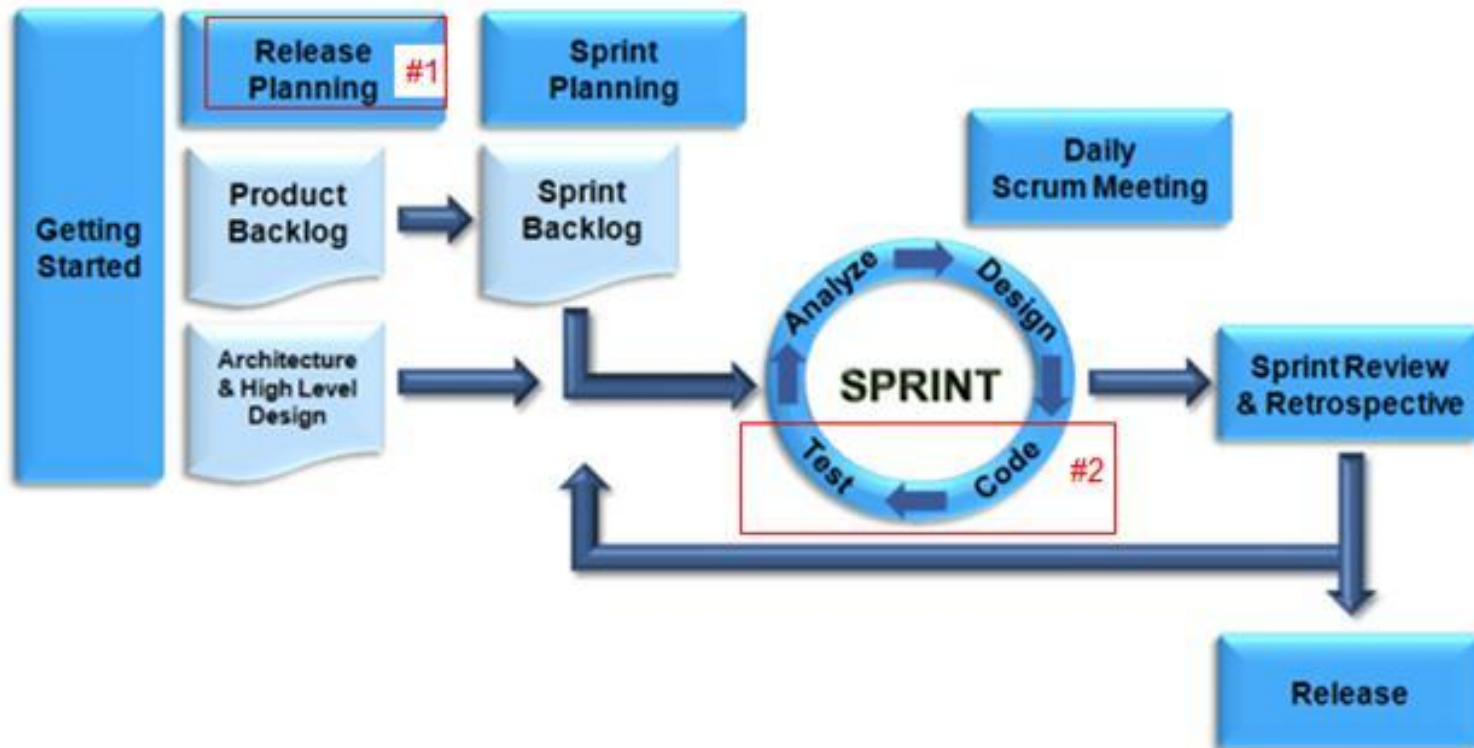
**Better to be a phase reviewer throughout, than a change ticket approver at the end**





# Agile SDL Checkpoints

- One Risk Assessment per Release (#1 on the diagram below)
- One Fortify scan per Sprint (#2 on the diagram below)



# Partnerships with Privacy, Legal, etc.

- Privacy – having EU representation on our privacy team has been crucial
- Data Architecture
- Legal – lead security/privacy attorney
- Compliance – strong alliance with compliance reps for each IT org
- Vendor Management Office (IPSA)
- Product Group CTO
- Corporate Governance
- Enterprise Architecture / SDLC (Dev tools, processes)
- Service Oriented Architecture team

**Having escalation points and allies in each of these areas has been essential**

# **Section Two**

# **Consultant Team**

# Security Consulting Staff Development

- Global reach – Brazil, India, Malaysia, and US
- Hot Market, Retention issues
- DB, App, and Network subject matter experts
- Weekly meetings
  - ▶ Global staff; 1:1 Manager / IC
  - ▶ Scheduled, unstructured, and informal “around the cubes” discussions
  - ▶ Collaborative team training
  - ▶ CISSP training group (3 rounds through Shon Harris)

**Onboarding deck and procedure docs  
for everything**

# Division of Labor for Security Consultants

- IT, Product Group, Services
- Mergers, acquisitions, and divestitures
- Interaction with Red Team
  - ▶ High-risk projects, at consultant's discretion
- Project management
  - ▶ Projects without a project charter—we don't say "no"
  - ▶ Informal project management within our team
- Outreach and Corporate Communications

**We have at least one SME dedicated to Apps, DB, and Network**

# Risk Modeler Tool, Risk Assessments, etc.

- This is our primary engagement mechanism, and it is the first security checkpoint in the SDLC.
- Spreadsheet approach was used prior to rollout of this tool
- Triage helps align most of our resources to high-risk projects
- Tool enhancements: Audit trail, Automated emails, Search
- On-the-fly question customization and weighted risk calculation
  - ▶ Engagement types with targeted questions (internal software, infrastructure, and vendor apps)
- Major factors in risk calculation weightings
  - ▶ Data Classification
  - ▶ Internally / Externally facing
  - ▶ SOX, PCI
- Low-risk - directed to self-help documentation and to our allies in compliance
- High-risk - usually have a security consultant in attendance at major project meetings/milestones, as well as penetration testing prior to launch
- Risk has impact on source code remediation requirements
- Need to mine data more deeply to follow up on some sorts of issues

**420 projects in 2008;  
726 projects in 2009;  
200 in Q1 2010**



# Threat Modeling

- **Initial emphasis on Product Group, Services during design phase**
- **Requires culture shift to doing Data Flow Diagrams**
- **Very time-consuming**
- **Resulting artifact is less important; having the conversation between security consultant and dev team is the key**
- **Dev lead or architect must attend**
- **CBA: Low-yield; 8-16 hours for 1-2 significant findings**
- **Adopting a light-weight threat modeling program for IT with a quiet rollout**
- **Using new MS Threat Modeling tool 3.1 for PG/Services**

**More experienced security consultants do this analysis intuitively**



# Source Code Scans

- **Manual versus automated (MS 200, Dell 10)**
- **Great vendor partnership**
- **Evolving procedures for which rules are enforced**
  - ▶ **Started with “top 5” hot issues**
    - XSS (MS Anti-XSS)
    - SQL Injection (Stored procedures, least privilege, input validation)
    - Buffer Overflow (C/C++, PG)
    - Hardcoded passwords (MS DPAPI)
    - Weak encryption (rare)
  - ▶ **Now all hot issues, as well as certain mediums**
    - Very little impact in sheer numbers after “top 5”
- **Back doors**
- **Exploring cloud-based scans for 3rd-party code**

**Plan to start modestly and tighten the screws as the program matures. Plan for exception management.**



# Pre-deployment Scans

- **Source code scans have a sweet spot. For high-risk apps, we have found a few additional issues via black/gray box testing**
- **May be our only option for languages/technologies not covered by source scans**
- **Host OS findings not in synch with enterprise patch windows / SLA's**
- **Entire Red Team in one time zone**
- **Most teams are ok with 1 week turnaround; recently, that has become an issue**
- **Must build remediation time into the project timeline**

**Risk-based, and at the consultant's discretion**

# Penetration Testing

- **Routine, regulatory requirement**
- **Scope is a moving target**
  - ▶ Acquisitions
  - ▶ New apps
  - ▶ 10,000 legacy apps
- **More thorough, manual testing by senior team members**
- **Opportunities for better coordination**

**The real challenge is not issue discovery, but remediation.**

# Lessons Learned

- **Adding ourselves into existing SDLC**
- **Partnering with other groups**
- **Leveraging regulatory compliance for adoption**
- **One step at a time, one org at a time, show metrics, build momentum**
- **Exception management process, executive escalation, roadmaps**
- **SDL@Dell won the ISE North America Information Security Project of the Year Award for 2008**

**We're doing fundamentals, not cutting edge work**

# Q & A, Suggestions for Improvement

■ **Michael\_Craigie [ @ ] dell.com**

**Thanks to Phil Agcaoili, Addison Lawrence,  
Chad Barker, Neil Matatall, and Brad Shaver for  
their review and input!**