Enterprise Application Security Practices: Real-world Tips and Techniques

L. Gustavo C. Barbato, Ph.D.

Maurício Pegoraro

Rafael Dreher

Agenda

Who we are…

How was built our SDLC…

How works our SDLC…

Who we are…

Our Information Security Organization

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.)

Security Consulting Staff

- 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

How was built our SDLC...

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

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

Addressing Global Standardization Issues

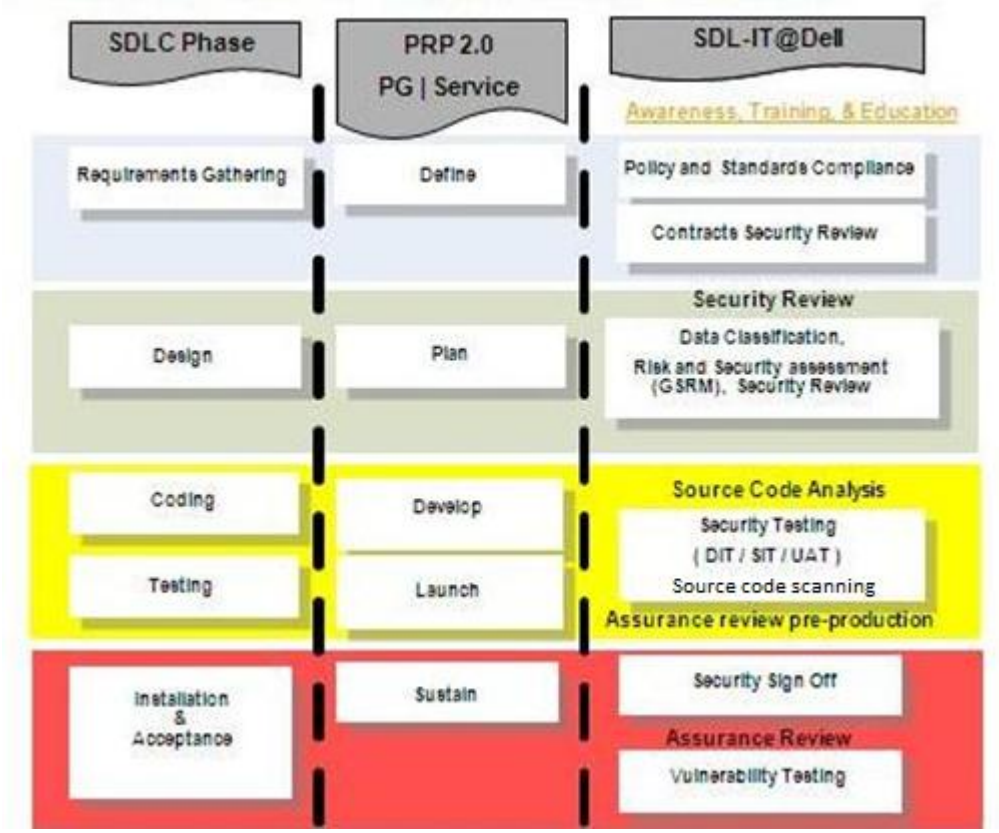
- Enterprise Architecture standards review board
- Multiple development frameworks
- Multiple development IDEs
- Multiple Operating Systems
- Multiple development languages
- Acquisitions and divestitures

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

How works our SDLC…

SDL Checkpoints in the SDLC

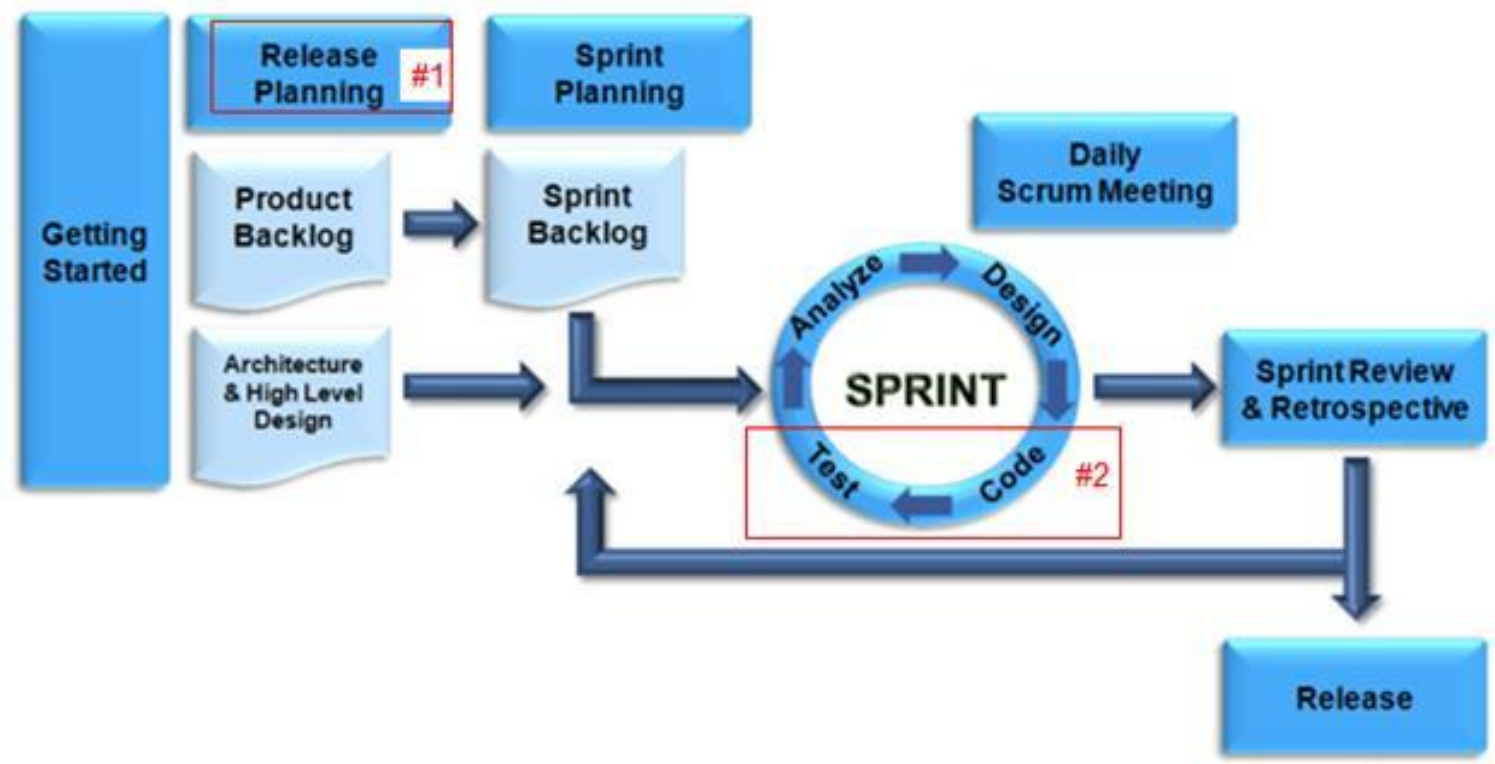
- Getting embedded early, with simple checkpoints
- IT / Services / Product Group tailoring
- Traditional versus Agile methods



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 source code scan per Sprint (#2 on the diagram below)



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

- Gustavo_Barbato [@] dell.com
- Mauricio_Pegoraro [@] dell.com
- Rafael_Dreher [@] dell.com

For more information:
http://www.owasp.org/images/e/ed/OWASP_AppSec_Research_2010_Real-World_Tips_by_Craigue.pdf