Case Study: Security Development Lifecycle at Microsoft

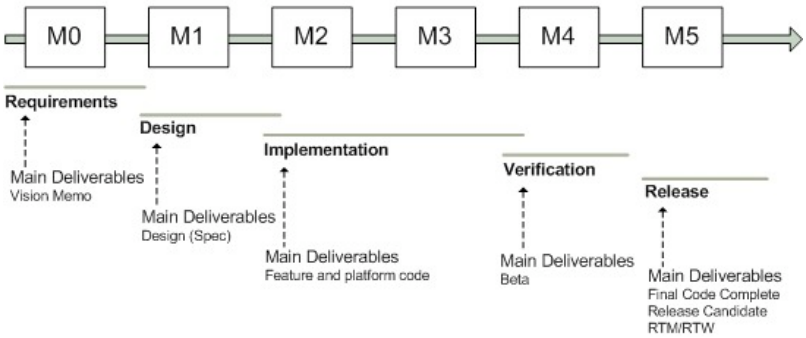
Origins

- Through Windows 2000 release
  - Secure Windows Initiative (SWI)
    - Expert resource for consulting and code reviews
- Through Windows XP release
  - SWI as company wide resource
    - Security training
    - Common tools
    - Team-wide "security days"
- Introduction of Trustworthy Computing
  - Windows (and other) security pushes
  - Focused reviews of designs, code, penetration resistance

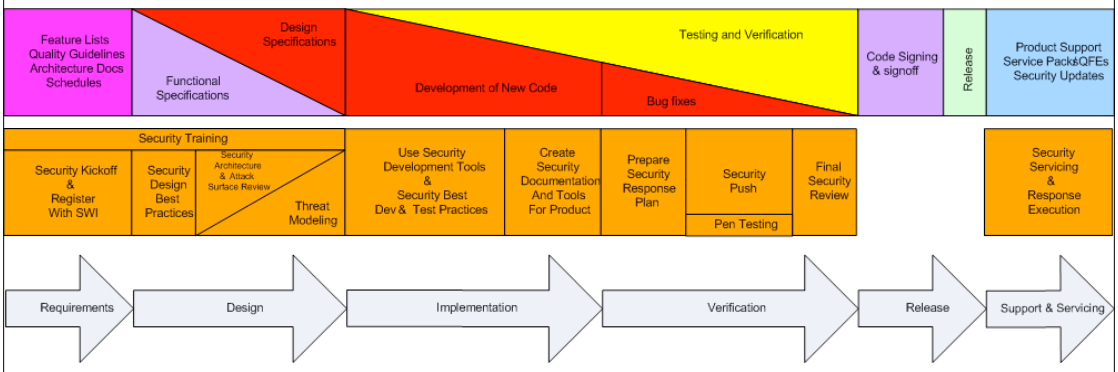
Where SDL Fits

Secure by Design	Threat modeling Code inspection Penetration testing
Secure by Default	Unused features off by default Reduce attack surface area Least Privilege
Secure by Deployment	Prescriptive guidance Security tools Training and education
Communications	Community engagement Transparency Clear policy

Traditional Baseline Process



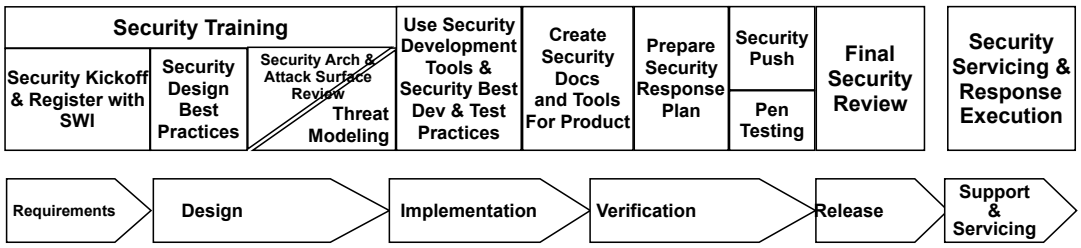
Integrating SDL into the development process



Requirements Phase

- Secure Windows Initiative (SWI) team assigns SWI Buddy
- Development team identifies security requirements
- SWI Buddy reviews product plan, makes recommendations, ensures resources are allocated by management
- SWI Buddy assesses security milestones and exit criteria
- (NOTE: This SWI Buddy will stay with the project through the Final Security Review)

Security Deployment Lifecycle Tasks and Processes



Design Phase

- Define and document security architecture
- Identify security critical components ("trusted base")
- Identify design techniques (e.g., layering, managed code, least privilege, attack surface minimization)
- Document attack surface and limit through default settings
- Create threat models and design countermeasures to mitigate threats
- Identify specialized test tools
- Define supplemental ship criteria due to unique product issues (e.g., cross-site scripting tests)
- Confer with SWI Buddy on questions
- Exit criteria: Design review complete and signed off by development team and SWI Buddy

Attack Surface Reduction Process (1 of 2)

- Look at all your entry points (the threat model helps)
- Primarily network I/O and File I/O
- Can any of the entry points' attack surface be driven lower?

ASR Process (2 of 2)

Higher Attack Surface	Lower Attack Surface
Executing by default	Off by default
Open socket	Closed socket
UDP	TCP
Anonymous Access	User Access
User Access	Admin Access
Internet Access	Local Subnet Access
SYSTEM	Not SYSTEM!

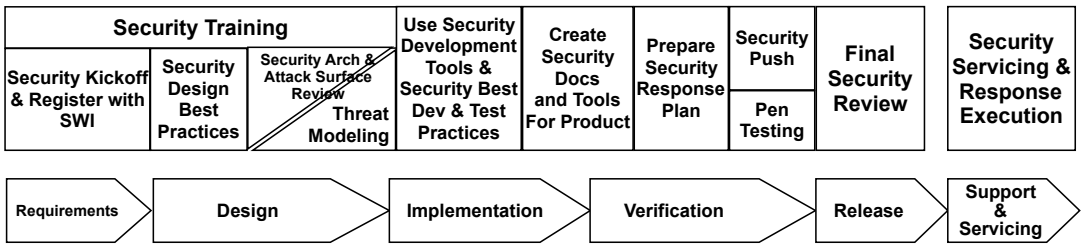
ASR Examples

- Windows XP SP2
  - Authenticated RPC
  - Firewall on by default
- IIS6
  - Off by default
  - Network service by default
  - Static files by default
- SQL Server 2005
  - xp_cmdshell off by default
  - CLR and COM off by default
  - Network service
- Visual Studio 2005
  - Web server localhost only
  - SQL Server Express localhost only

How ASR Helped

- Sasser
  - Affected Win2000 and WinXP
  - Did not affect Win2003
    - RCP endpoint was marked local admin only
- Zotob
  - Affected Win2000
  - Did not affect WinXP
    - Firewall & authenticated RPC

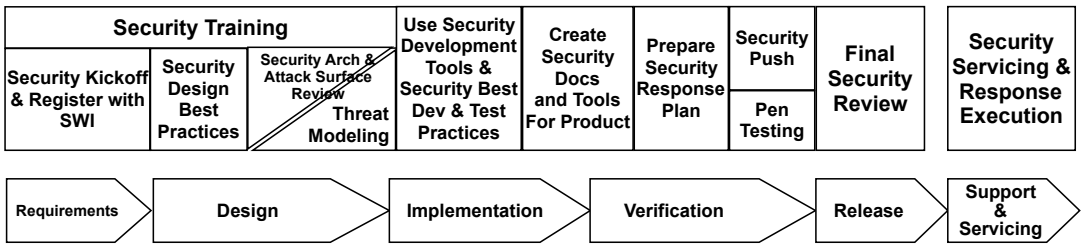
Security Deployment Lifecycle Tasks and Processes



Development Phase

- Apply coding and testing standards (e.g., safe string handling)
- Apply fuzz testing tools (structured invalid inputs to network protocol and file parsers)
- Apply static code analysis tools (e.g., to find buffer overruns, integer overruns, uninitialized variables)
- Conduct code reviews

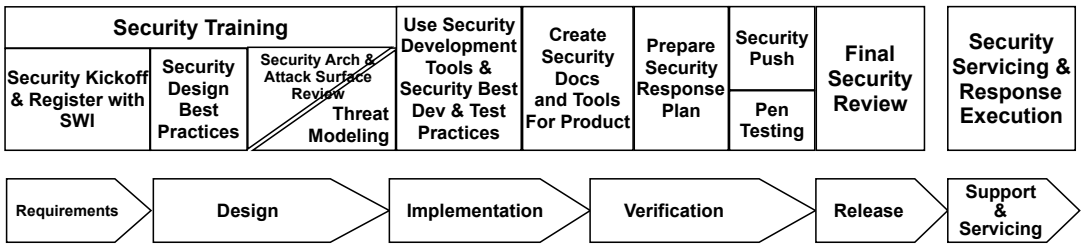
Security Deployment Lifecycle Tasks and Processes



Verification Phase

- Software functionality complete and enters Beta
- Because code complete, testing both new and legacy code
- Security Push
  - Code reviews (especially legacy/unchanged code)
  - Penetration and other security testing
  - Review design, architecture, threat models in light of new threats

Security Deployment Lifecycle Tasks and Processes



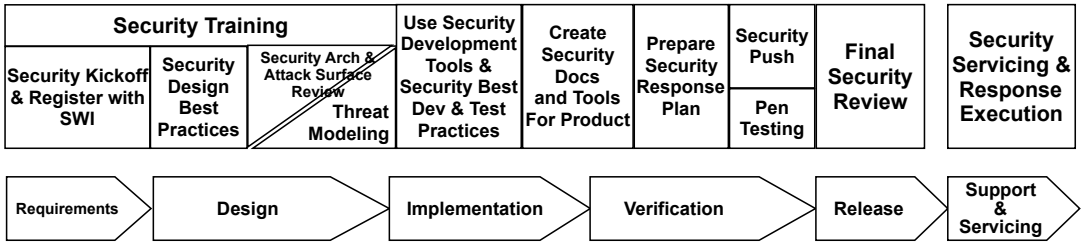
Final Security Review (FSR)

- "From a security viewpoint, is this software ready to deliver to customers?"
- 2-6 months prior to software completion
- Software must be in a stable state with only minimal non-security changes expected prior to release
- FSR results: If the FSR finds a pattern of remaining vulnerabilities, revisit the earlier phases and take pointed actions to address root causes (e.g., improve training, enhance tools)

What is FSR?

- Completion of a questionnaire by the product team
- Interview by a security team member assigned to the FSR
- Review of bugs that were initially identified as security bugs, but on further analysis were determined not to have impact on security, to ensure that the analysis was done correctly
- Analysis of any newly reported vulnerabilities affecting similar software to check for resiliency
- Additional penetration testing, possibly by outside contractors to supplement security team

Security Deployment Lifecycle Tasks and Processes



Response Phase

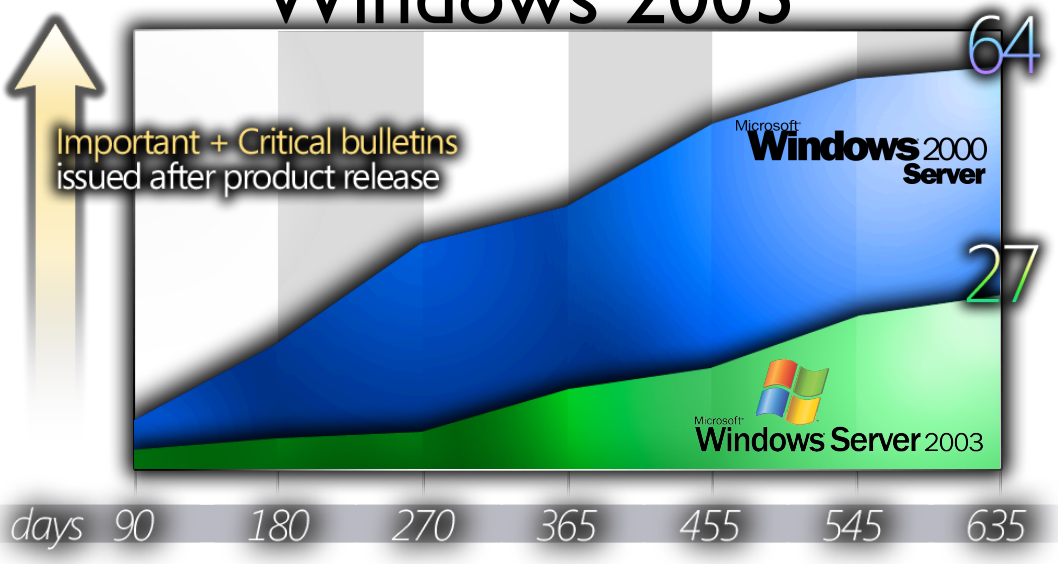
- Microsoft Security Response Center
- Patch Management
- Post Mortems and feedback to the SDL

Education For The SDL

- training staff as a part of New Employee Orientation
- training staff as part of a security push
- training developers, testers, program managers, user education staff and architects annually
- funding academic curriculum development through Microsoft Research
- publishing material on writing secure code, threat modeling, and SDL and offers courses (see http://www.microsoft.com/learning)

Results

SDL Results: Windows 2003



Source: Microsoft Security Bulletin Search

SDL Results: Office 2003

Office Bulletins since Office 2003 shipped (Aug 2003)

12

4

All Office Bulletins since ship 8/03

Affecting Office 2003

Bulletins after August 2003:
(* affected Office 2003)

- September: MS03-035, MS03-036, MS03-037, MS03-038
- November: MS03-050

2004

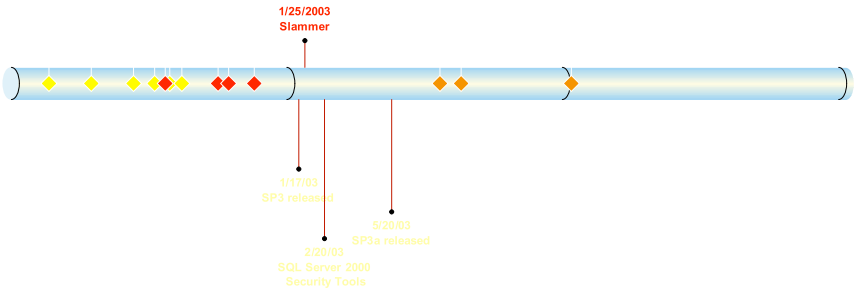
- October: MS04-033
- September: MS04-028* (GDI+ issue) …
- September: MS04-027* (WordPerfect converter)
- March: MS04-009

2005

- February: MS05-005
- February: MS05-012* (OLE issue) …
- April: MS05-023* (Word buffer overflow)

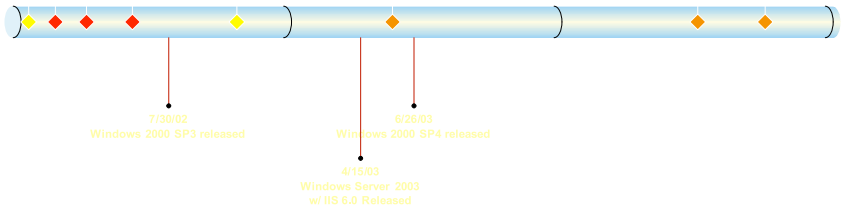
SDL Results: SQL Server

SQL Server 2000
2002-2005 (YTD)



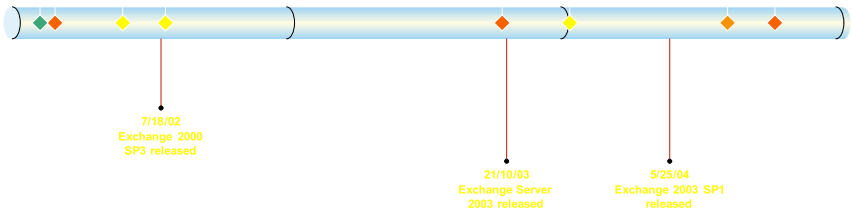
SDL Results: IIS 4.0, 5.0, 5.1, 6.0

IIS 4.0, 5.0, 5.1, 6.0
2002-2005 (YTD)



SDL Results: Exchange

Exchange 5.0, 5.5, 2000, 2003
2002-2005 (YTD)



Credits

This presentation is based on material from the following:

- "Security Development Lifecycle: Changing the Software Development Process to build in Security from the start" presentation by Eric Bidstrup & Ellen Cram Kowalczyk, Security Business and Technology Unit, Microsoft Corporation