



Microsoft Security Fundamentals

Andrew Cushman

Director Security Engineering & Community

Contact: [andrewcu at microsoft dot com](mailto:andrewcu@microsoft.com)

Intro – Who am I?



- Director of Security Community
 - Outreach to Community
 - Community Advocate / Ombudsman w/in MS
- 16 year MS veteran – 7 years on IIS
- Responsible for Code Red and Nimda
 - Rejected MSADC vdir defaults change for IIS5
- Responsible for IIS 6 security
 - Group manager – IIS6 Engineering Team
 - Hired @stake for Pen Test engagement

Agenda – Why am I here?



- Describe the MS security fundamentals
 - How we got here – a brief review
 - Our holistic approach – the security development lifecycle
 - Specific examples that show our work
- 3 things I want you to take away
 - We “Get it”
 - MS understands the industry wide security problems
 - And that Security requires industry wide solutions
 - We “Walk the Walk”
 - We are delivering excellent results - Maybe not perfect, but reasonable and industry leading
 - We’ re in it for the long haul
 - MS committed to long term security investments
 - Security Is a journey – it’s not a destination



PART 1: WE GET IT

Brief History



- MSRC creation and early years
- SWI (Secure Windows Initiative)
 - 2 guys in their spare time
- TwC memo from Chairman Bill
- Code Red, Nimda, Blaster, Slammer...
- Security Community Outreach ('03 party at Black Hat)
- Windows XP sp2
- Windows Vista

Today's Changed Ecosystem



- Security Industry Matures
 - Expanding number of tools & experts & researchers
 - Low barrier to entry attracts new entrants
 - More researchers & more areas = lots more bugs
- New actions & patterns & criminal presence
 - AdWare and SpyWare
 - The rise of botnets and botherders
- Attacks are constant and targeted
 - Move toward targeted attacks
 - News reports of corporate and government espionage
- Still on the upswing
 - Unlimited researcher creativity & new attack surface
 - New attack classes and vectors

The Changing Ecosystem



“Indictments were filed by an Israeli prosecutor against nine men in the industrial espionage case that involved planting Trojan horses on rival companies' computers to spy out their secrets.”

InformationWeek
July 8, 2005

“Security experts have revealed details about a group of Chinese hackers who are suspected of launching intelligence-gathering attacks against the U.S. government.”

Alan Paller,
SANS Institute in ZDNet
November 23, 2005

“Foreign governments are the primary threat to the U.K.'s critical national infrastructure because of their hunger for information, a British government agency said.”

Roger Cummins
NISCC Director in ZDNet
November 22, 2005

“You will see less shotgun types of attacks and more stealthy kinds of attacks going after financial information because there are whole new sets of ways to make money ”

Amrit Williams
Research Director at Gartner – Reuters
February 13, 2006

Top Security Challenges



- Security Researchers & ISVs at odds
 - Customers safety is a common goal, but
 - Disagreement on tactics
- Security Researchers distrust Software ISVs
 - No consensus on Responsible Disclosure
 - Differing views of benefit of Exploit code and PoC
- Changed economic landscape
 - Vulns have value in an above ground economy
 - Attribution in Bulletins losing value in new economy
- Changed Threat Landscape
 - Shrinking delta btw publish and exploitation
 - Vuln Full Disclosure increases customer risk



PART 2:

HOLISTIC APPROACH - SDL

Security Focus: Microsoft Corporation



Vision:

A secure platform strengthened by security products, services and guidance to help keep customers safe



- Excellence in fundamentals
- Security innovations



- Scenario-based content and tools
- Authoritative incident response



- Awareness and education
- Collaboration and partnership

Security Engineering & Communications



The Security Fundamentals Group at Microsoft

One team responsible for Microsoft's

- Security Development Lifecycle
- Security Engineering (Eng. Standards)
- Penetration Testing (Std. Enforcement)
- Security Response & Updates
- Emergency Incident Response
- Community Outreach

Security Focus: Sec Fundamentals Group



Vision:

Embed industry leading security in the Microsoft development culture and in every MS product and service



- Cutting edge Research - /GS
- Heap mitigations
- Fuzzing
- Analysis Tools
- Patchguard

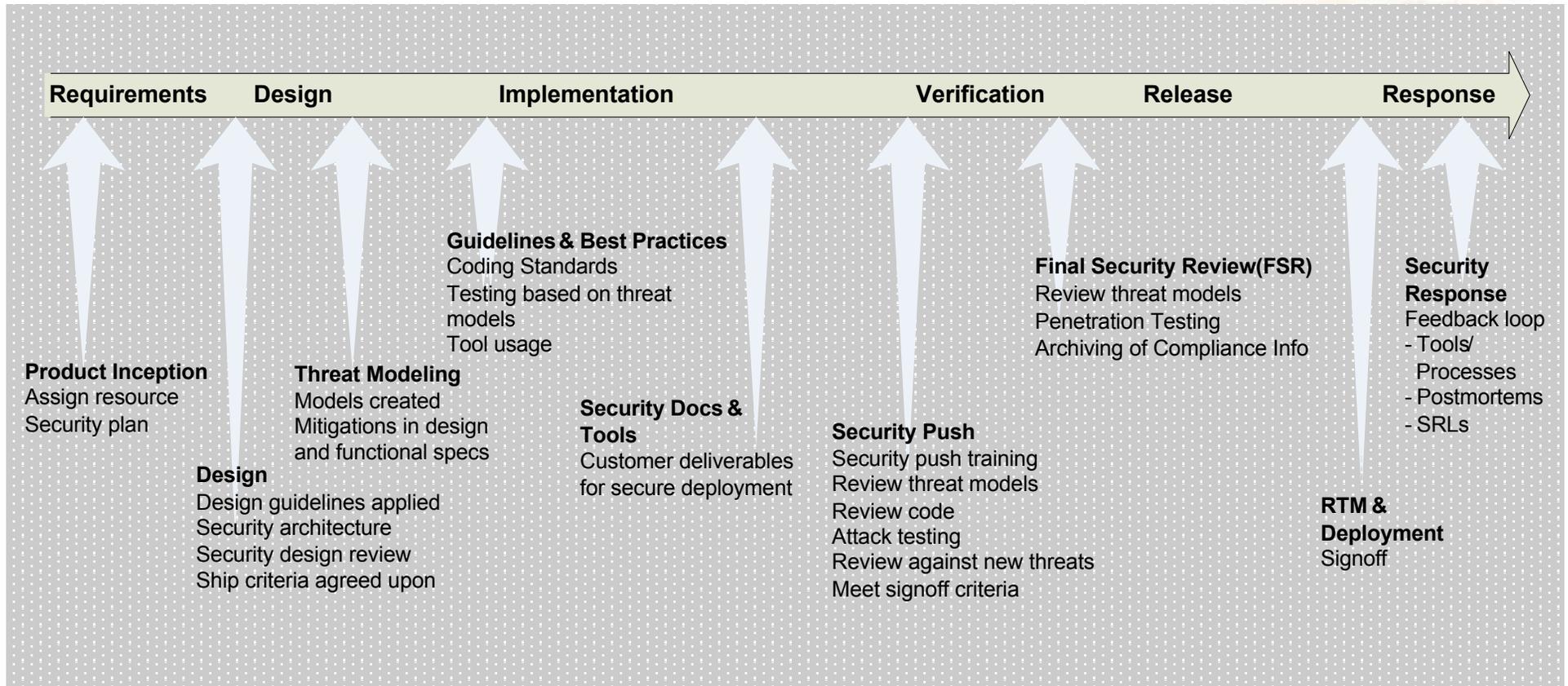


- SDL article on MSDN
- MSRC Bulletins
- Security Advisories
- Conf. Presentations
- Internal Training
- SWI KB

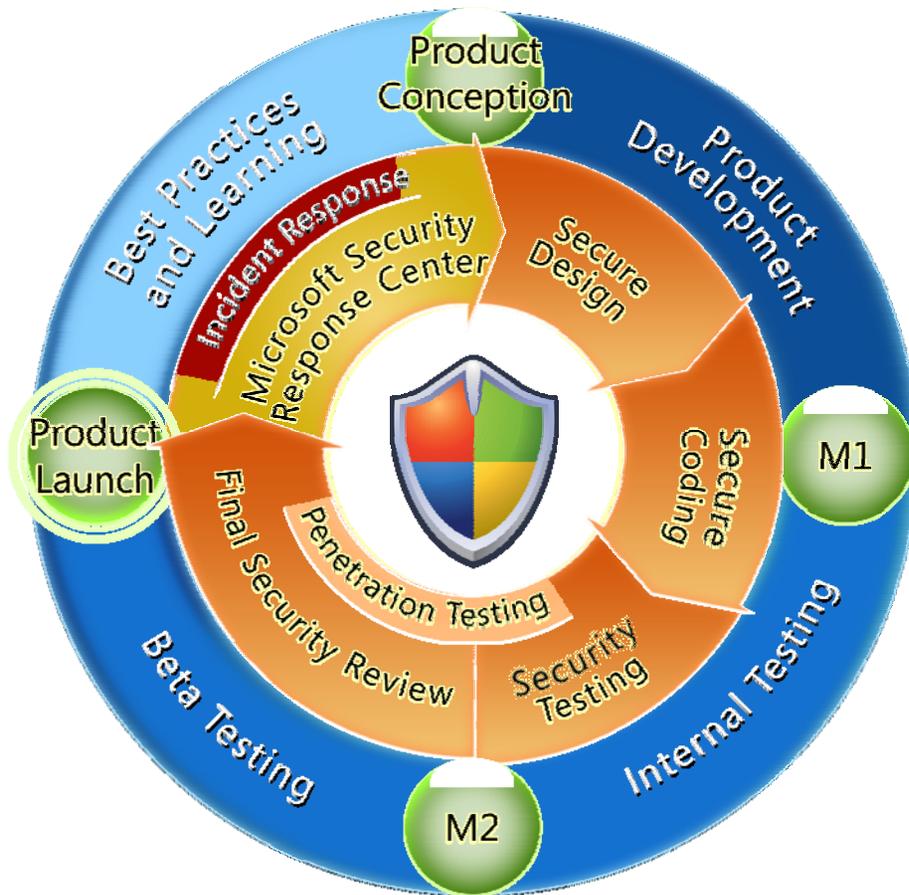


- Conf. sponsorship
- CERT collaboration
- MSRA
 - VIA (Virus ISVs)
 - GIAIS (ISPs)
- BlueHat

Security Development Lifecycle



Security Development Lifecycle



Process

- Defines security requirements and milestones
- **MANDATORY** if exposed to meaningful security risks
- Requires response and service planning
- Includes Final Security Review (FSR) and Sign-off

Education

- Mandatory annual training – internal trainers
- BlueHat – external speakers on current trends
- Publish guidance on writing secure code, threat modeling and SDL; as well as courses

Accountability

- In-process metrics to provide early warning
- Post-release metrics assess final payoff (# of vulns)
- Training compliance for team and individuals

- Microsoft Product Development Lifecycle
- Microsoft Security Development Lifecycle

SDL and Microsoft Products



- **SDL applies across all Divisions and Businesses**
 - Defines Incident Response & Update Requirements & Guidelines
 - Defines Engineering Requirements and Guidelines
 - Validation To Ensure Standards Are Met
- **Final product security profile combines**
 - Customer requirements
 - Deployment and Usage requirements and
 - Security Requirements
- **Products must pass Final Security Review to ship**

Microsoft Security Training Courses



2003 - Security Basics was the only class

2006 – Expanded general & specific offerings

- Introduction to the SDL and Final Security Review (FSR) Process
- Basics of Secure Software Design, Development, and Test
- Threat Modeling
- Security for Management
- Classes of Security Defects
- Defect Estimation and Management

Developers

- Secure Coding Practices
- Security Code Reviews

Testers & Program Managers

- Introduction to Fuzzing
- Implementing Threat Mitigations
- Time-tested Security Design Principles
- Attack Surface Reduction and Analysis

2007 and beyond – Continual and Ongoing effort

External Training : BlueHat Conference



- Education on current threats & trends
 - 1st day for execs – condensed sessions
 - 2nd day for engineers – in depth sessions

March '05

- Dino Dai Zovi & Shane McAuley
- Matt Conover
- HD & Spoonm
- Dug Song
- Dan Kaminsky

October '05

- Skape
- Vinnie Liu
- Dave Maynor
- Brett Moore
- Toolcrypt

External Training : BlueHat Conference



- Expanded to 3 days in March 2006
 - 1st day for execs – condensed sessions
 - 2nd day focused on SQL and Web Apps
 - 3rd day general topics and Windows Vista

March '06

- David Litchfield
- Alexander Kornbrust
- Johnny Long
- Caleb Sima
- HD Moore
- Kev Dunn

March '06

- Halvar Flake
- HD Moore
- Scott Stender & Alex Stamos
- Dan Kaminsky & Josh Lackey

Security Community Outreach



- Why bother?
 - Dialog leads to understanding and (hopefully) cooperation
 - Community & MS collaboration can deliver more secure products
- What is it?
 - Community Ombudsman w/in MS
 - Advocate & strategist for MS participation in Community
- How
 - Listen, participate, and close the feedback loop
 - Attend Conferences
 - Suggest speakers and content
 - Internal activities & education - BlueHat, mini-summits
 - Foster durable relationships

Security Community Outreach



Listen, Participate & close the loop w/ the Community

- Engage the community
 - Personalize the engagement w/ a faceless company
 - Put a face on “hacker threat” for MS execs & engineers
- Technical Innovation
 - Conference Attendance for cutting edge research
 - Facilitate knowledge transfer to the product groups
- Participate in the Community
 - Conference co-sponsorship
 - Contribute to the advancement of security science
- Guidance
 - Connect experts in Product teams & Security Community
- Promote Responsible Disclosure e.g.,
 - Encourage dialog btw researchers & Vendors
 - Our Goal: Coordinated release of vuln details & updates

Security Response Process



Security Bulletin Release Process

Repeatable, Consistent, Process

High Quality Product Updates

Authoritative Accurate Guidance

Security Incident Response Process

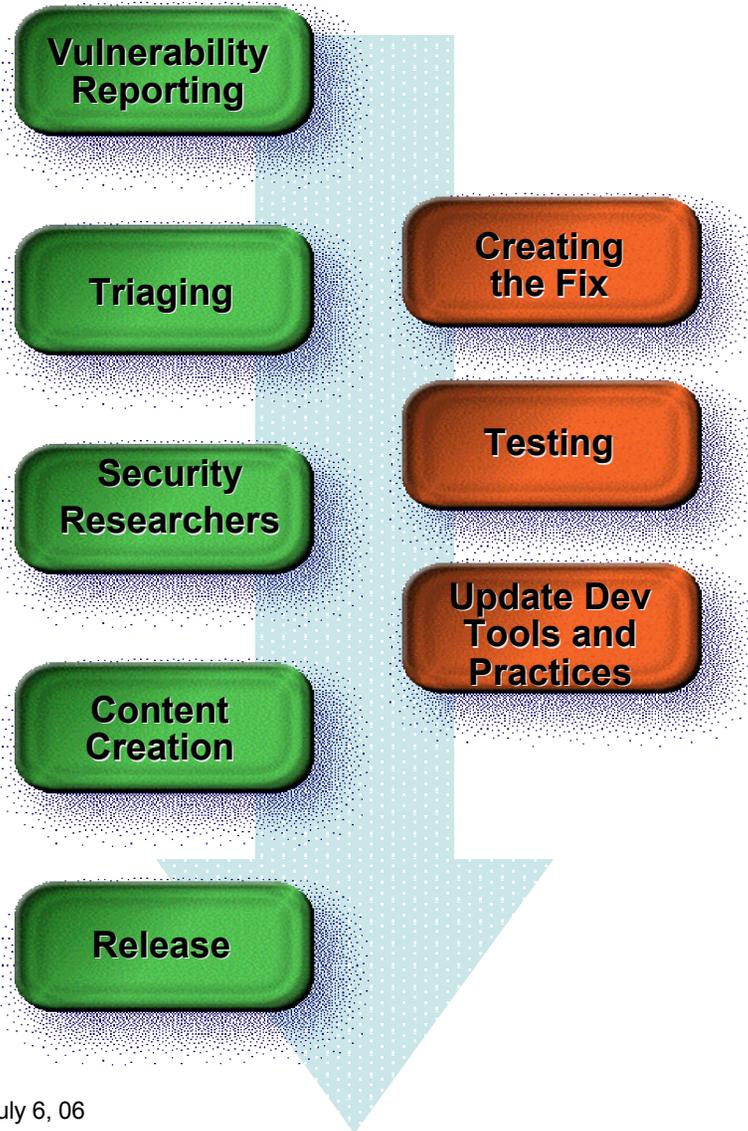
Timely and Relevant Information

Mitigations and Protection

Solution and Guidance

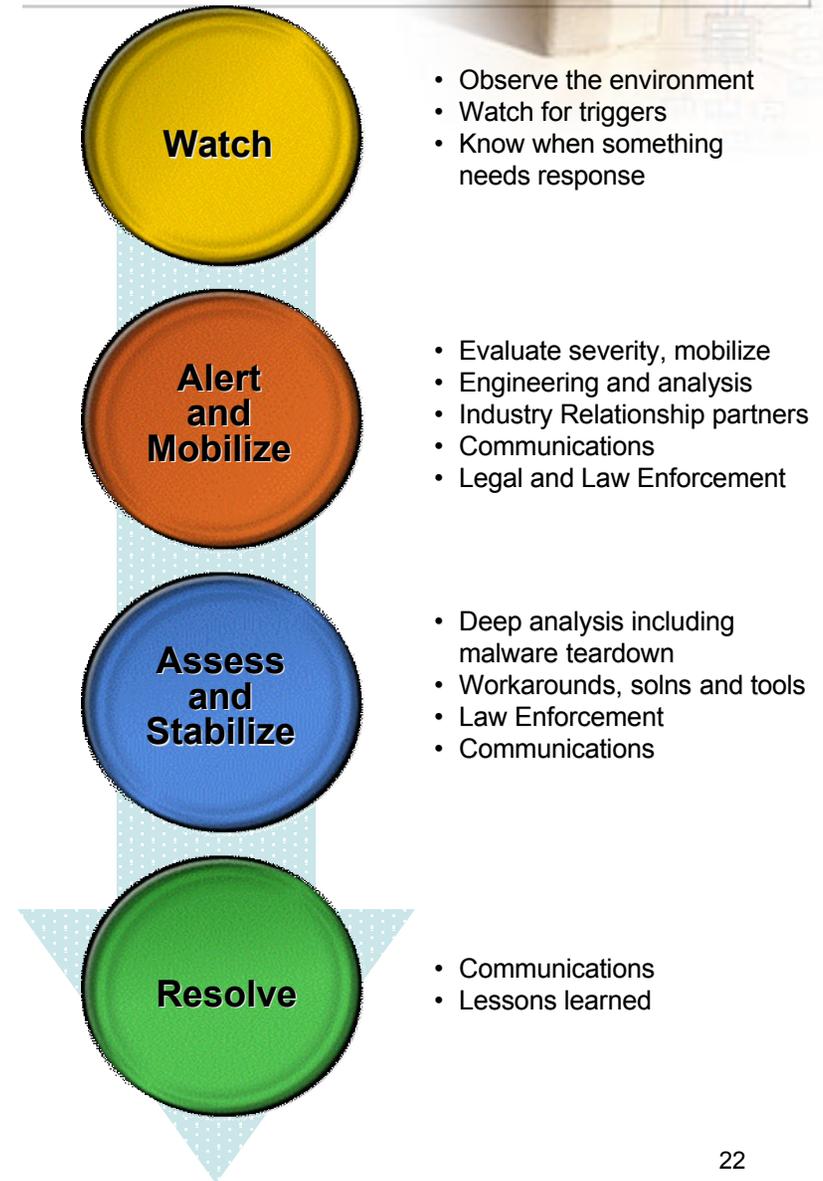
Security Response

Monthly Response Process



July 6, 06

SSIRP Incident Response



22



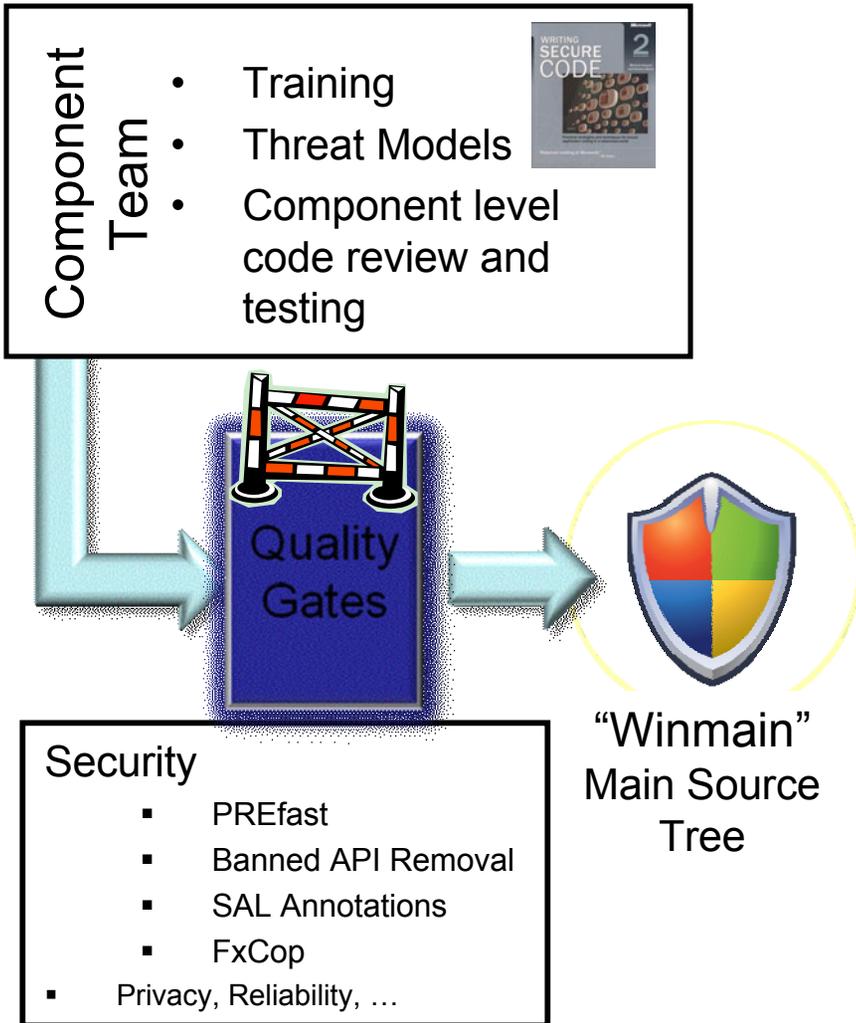
PART 3: RESULTS

Case Study: Windows Vista



- Security Design and Architecture
 - Service Hardening
 - Attack Surface reduction
 - UAC/ IE Protected Mode
- Consistent standards and application: Security Basics
 - Many SDL recommended best practices become required engineering tasks
 - Banned API removal
 - Banned crypto removal
 - SAL for ALL headers
- Automation
 - Engineering Tools
 - Testing tools
- New Engineering Processes & Standards
 - ALL new features required threat model along with Design, Spec, and Test Plan
 - Central Privacy team and Privacy Quality Gate
- Security Expertise Applied to High Risk code
 - Parser Fuzzing
 - Security Experts for Feature reviews and Pen testing

In XA STAM



High Risk Code Across All Code

Security Bug Tracking

PREfix, Default Permissions

Design & Attack Surface Review

In Depth Threat Model Review

Penetration Testing

Mini-Security Push (if necessary)

Network and File Parser testing

Special Cleanup Projects

Case study: WMF – from fix to release



Coding the Fix

- The team isolated the bug quickly
- Built update, Smoke tested and then deliver to test team

Functional / Regression testing:

- More than 450,000 individual GDI/User test cases
- Approximately 22,000 hours of stress
- Over 125 malicious WMF's verified to be fixed by the update
- Over 2,000 WMFs from our image library analyzed
- Approximately 15,000 Printing specific variations run & 2,800 pages verified

Application Compatibility Testing:

- Over 400 Applications tested
- Across all 6 supported Windows platforms

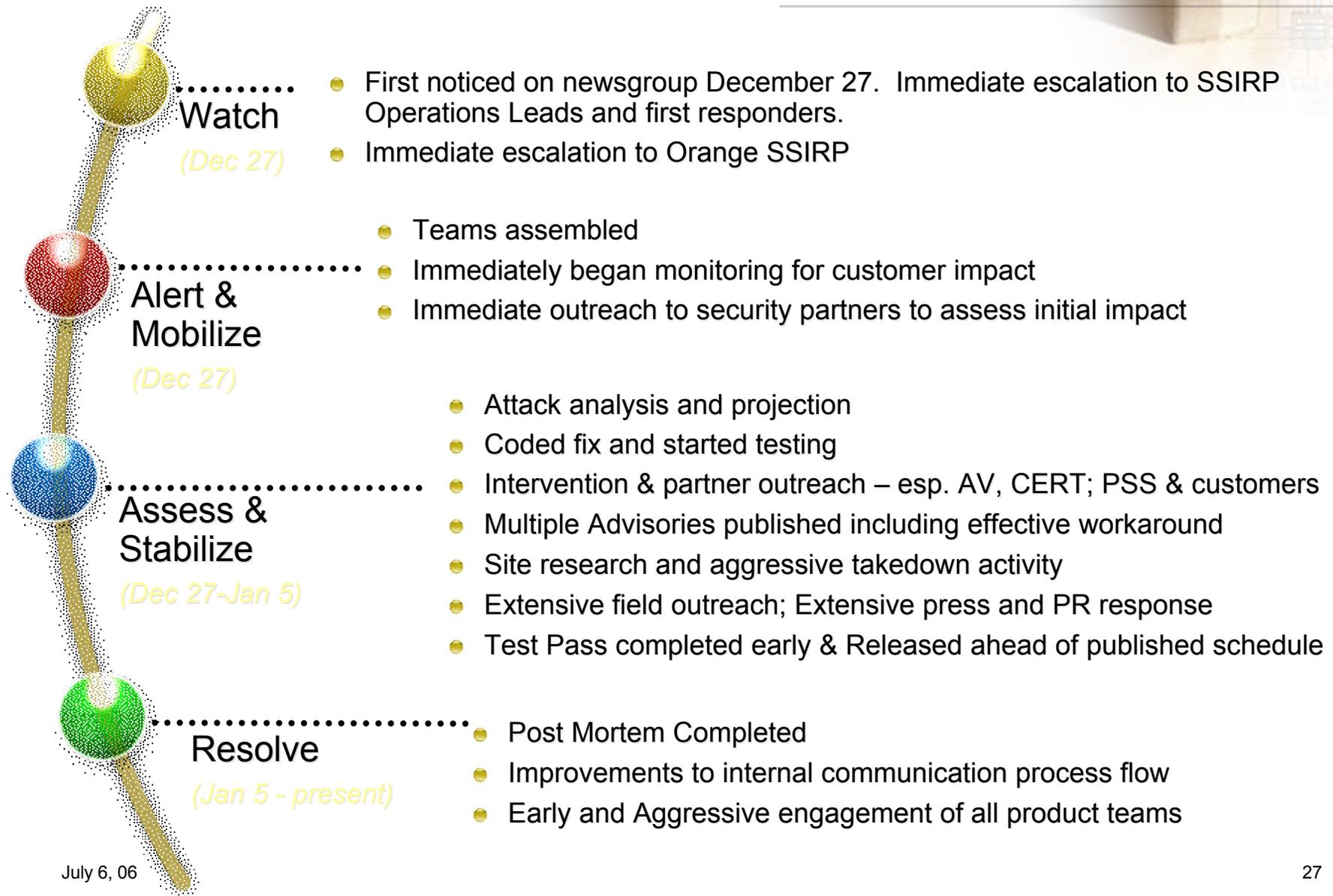
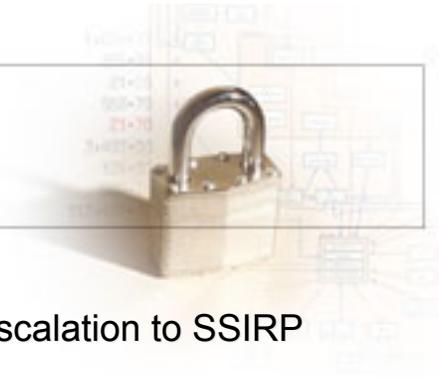
Security Update Validation Program

- For broad coverage of LOB application compatibility and deployment
- International coverage

Deployment tools:

- MBSA 1.2, MBSA 2.0, Microsoft Update/Windows Update, AutoUpdate, Software Update Service (SUS/WSUS), SMS

Case Study: WMF Background

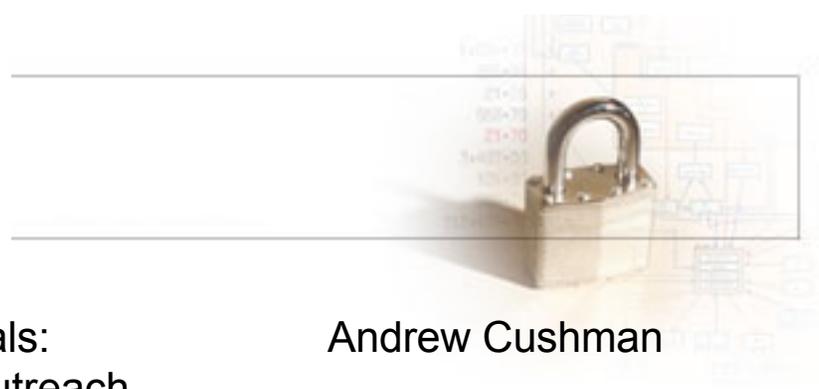


Conclusion



- Microsoft has made a lifestyle commitment – not a perennial new year’s resolution
- Your company / organization can do this too
 - Requires exec support
 - Requires critical mass of experts and funding
- Give us feedback – we’re listening!
 - This is a dynamic process. We continually strive to improve

Still to Come!



| | | |
|---------------|--|------------------------------------|
| 09:00 – 09:50 | Microsoft Security Fundamentals: Engineering, Response and Outreach | Andrew Cushman |
| 10:00 – 11:00 | Security Engineering in Windows Vista | John Lambert |
| 11:15 – 12:30 | The NetIO Stack: Reinventing TCP/IP in Windows Vista | Abolade Gbadegesin |
| 13:45 – 15:00 | WiFi in Windows Vista: A Peek Inside the Kimono | Noel Anderson & Taroon Mandhana |
| 15:15 – 16:30 | Windows Vista Heap Management Enhancements – Security, Reliability and Performance | Adrian Marinescu |
| 16:45 – 18:30 | Case Study: The Security Development Lifecycle and Internet Explorer 7 | Tony Chor |



secure@microsoft.com

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.