

Inside The Microsoft Security Response Process

Security Response Marketing
Security Business and Technology Unit

Microsoft Security Response Center

Investigate and Resolve Vulnerability Reports

- Staff public reporting alias
- Monitor security lists
- Single point of coordination and communications

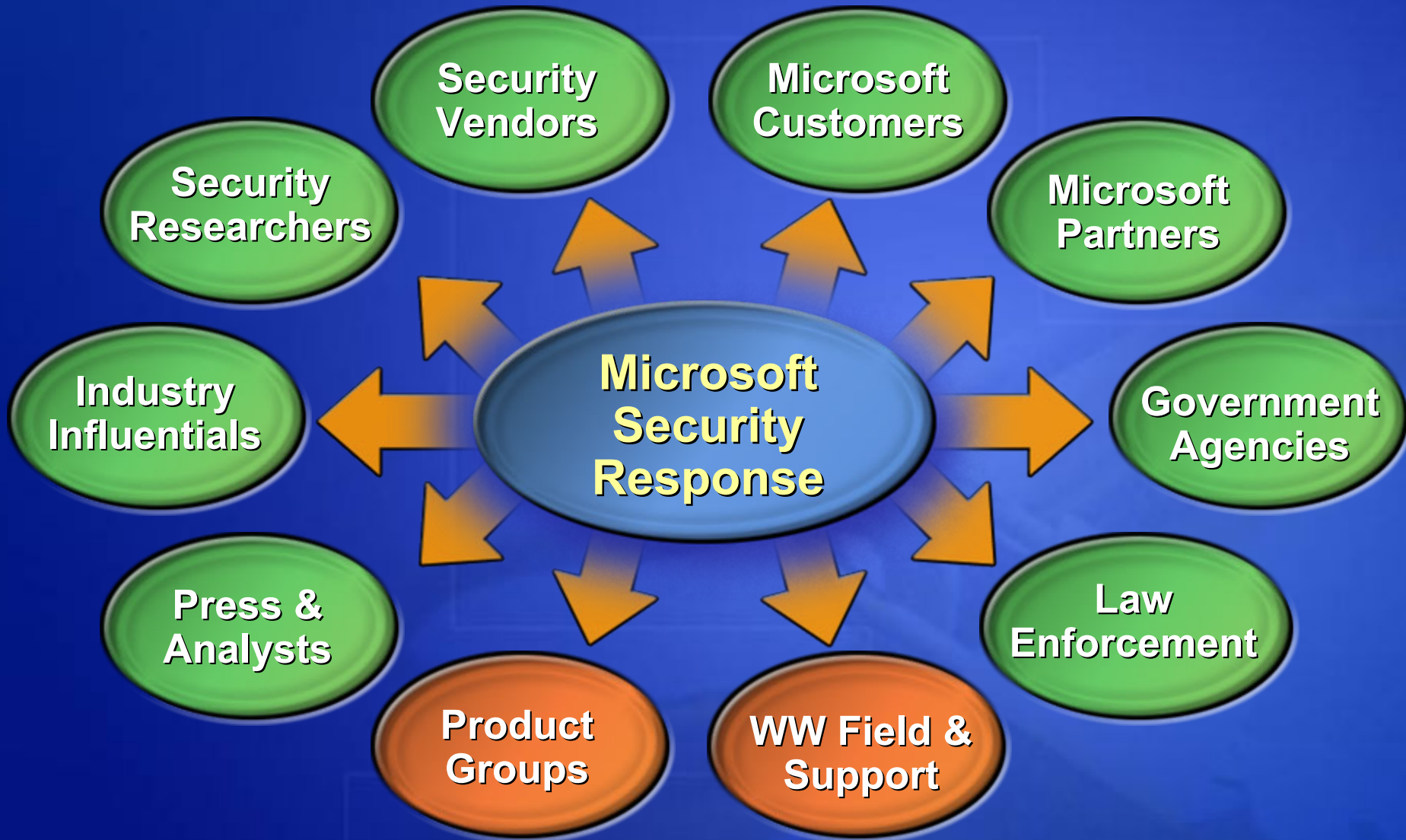
Microsoft Security Response Process

- Own and coordinate company wide process
- Work to prevent issues through security engineering and development process changes

Building Relationships and Communications

- Work with law enforcement and industry influentials
- Create community with vulnerability finders

World Wide Outreach



Building A Security Response Process

Security Bulletin Release Process

Build a more Simplified,
Manageable Process

Enhance and Improve
Bulletin Content

Expand Resources
and Support

Security Incident Response Process

Provide Timely and
Relevant Information

Help Mitigate and Protect

Deliver Solution to Resolve

Releasing A Security Update

Vulnerability Reporting

- MSRC receives incoming vulnerability reports through:
 - Secure@Microsoft.com – Direct contact with MSRC
 - Microsoft TechNet Security Site – anonymous reporting
- MSRC responds to all reports:
 - 24 hour response Service Level Agreement to finder
 - Internal response can be immediate when required

Triaging

- Assess the report and the possible impact on customers
- Understand the severity of the vulnerability
- Rate the vulnerability according to severity and likelihood of exploit, and assign it a priority

Creating the Fix

- SWI and Product Team:
 - Investigate the impact of the vulnerability
 - Search for other variants
 - Conduct further investigation of surrounding code and design
- Generate fix for Test

Managing Finder Relationship

- Establish communications channel
 - Quick response
 - Understand motivation and needs
 - Regular updates
- Build the community
- Encourage responsible reporting

Testing

- Several levels of testing:
 - Setup and Build Verification
 - Depth
 - Integration and Breadth
 - Microsoft Corporate network
 - Controlled beta

Content Creation

- Write security bulletin, including:
 - Affected software/components
 - Technical description
 - Workarounds and Mitigations
 - FAQs
 - Acknowledgments
- Get product group sign-off

Update Dev Tools and Practices

- Update best practices to avoid repeating errors in the future
- Update testing tools
- Update development and design process

Release

- Release security bulletins on the second Tuesday of every month
- Coordinate all content and resources going live
- Push information and guidance out to customers
- Monitor customer issues and press activities

Bulletin Severity Ratings

Critical

Exploitation could allow the propagation of an Internet worm without user action

Important

Exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources

Moderate

Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation

Low

Exploitation is extremely difficult, or whose impact is minimal

More information: www.microsoft.com/technet/security/bulletin/rating.msp

Outreach And Communications

Pre Release

- Security Bulletin Advance Notification - three business days prior to release

Second Tuesday Release Day

- Updates posted on Download Center, Windows Update and/or Office Update
- Customer email notifications sent
- Bulletins posted on Microsoft websites
- Proactive Press and PR outreach
- Security newsgroups posting

Post Release

- Security Bulletins Webcast (Wednesday following release, 11AM PT)
- Monitor bulletin uptake and customer issues through PSS and Windows Update
- Bulletin maintenance

Security Incident Response

Overview

SSIRP - Software Security Incident Response Plan

- Companywide process to deal with critical security threats
- Mobilize Microsoft resources worldwide
- Goals:
 - Quickly gain a thorough understanding of the problem
 - Provide customers with timely, relevant, consistent information
 - Deliver tools, security updates and other assistance to restore normal operation

Responding To A Security Incident

Watch

- Observe environment to detect any potential issues
- Leverage existing relationships with:
 - Partners
 - Security researchers and finders
- Monitor customer requests and press inquiries

Alert and Mobilize

- Convene and evaluate severity
- Mobilize security response teams and support groups into two main groups:
 - Emergency Engineering Team
 - Emergency Communications Team
- Start monitoring WW press interest and customer support lines for this issue

Assess and Stabilize

- Asses the situation and the technical information available
- Start working on solution
- Communicate initial guidance and workarounds to customers, partners and press
- Notify and inform Microsoft sales and support field

Resolve

- Provide information and tools to restore normal operations
- Appropriate solution is provided to customers, such as a security update, tool or fix
- Conduct internal process reviews and gather lessons learned

Case Study: Sasser



Watch

(Apr. 13-28
2004)

- Microsoft releases security bulletins for April, including MS04-011 which addresses a vulnerability in LSASS
- Start monitoring customer help lines, newsgroup & community activities and press inquiries

Alert & Mobilize

(Apr. 29 2004)

- First reports of Sasser coming in
- Alert security response teams and pull people into the emergency engineering and communications rooms

Assess & Stabilize

(Apr. 30 - May 3 2004)

- Start analyzing technical details and work on solution (cleaner tool)
- Initial guidance communicated to customers
 - Sasser landing page off of www.microsoft.com/security
 - Email alerts sent through the security notification services
- Send out partner and WW field alerts
- Sasser Worm Removal Tool v1.0 released to Download Center

Resolve

(May 4-10 2004)

- Sasser Worm Removal Tool v2.0 released to Windows Update
- Massive customer and partner communication to help clean systems:
 - Sasser Technical Webcast
 - Online support chats
 - Updated Microsoft websites
- Removal tool continuously updated to clean for new variants

Resources

- Microsoft Security Web site: www.microsoft.com/security
- Sign up to receive e-mail about security updates: www.microsoft.com/security/bulletins/alerts.mspx
- Sign up for the Security Bulletin Web cast: www.microsoft.com/technet/security/bulletin/summary.mspx
- Security Bulletins Search: www.microsoft.com/technet/security/current.aspx
- Security Guidance Center for Enterprises: www.microsoft.com/security/guidance
- Protect Your PC: www.microsoft.com/protect

The Microsoft logo is centered on a blue background. It features the word "Microsoft" in a white, bold, italicized sans-serif font. A registered trademark symbol (®) is located at the top right of the word. The background is a solid blue color with a faint, large-scale grid pattern and a subtle image of a person's hands holding a device.

© 2003 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.