Vulnerability Management Best Practices

Eric Levin

VP Product Marketing, Qualys Inc.

June 2004

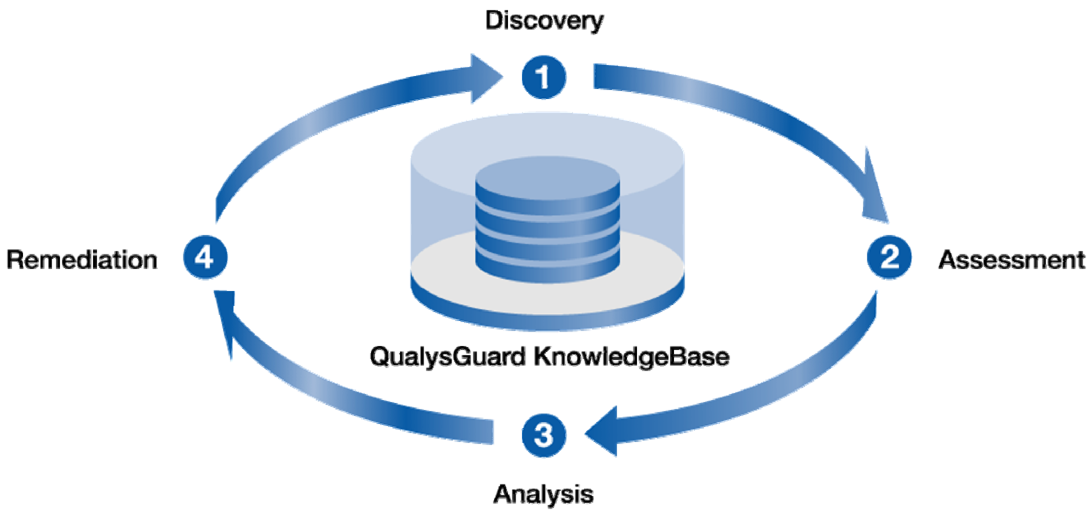
EMPOWERING SECURITY. ENABLING COMMERCE.

Agenda

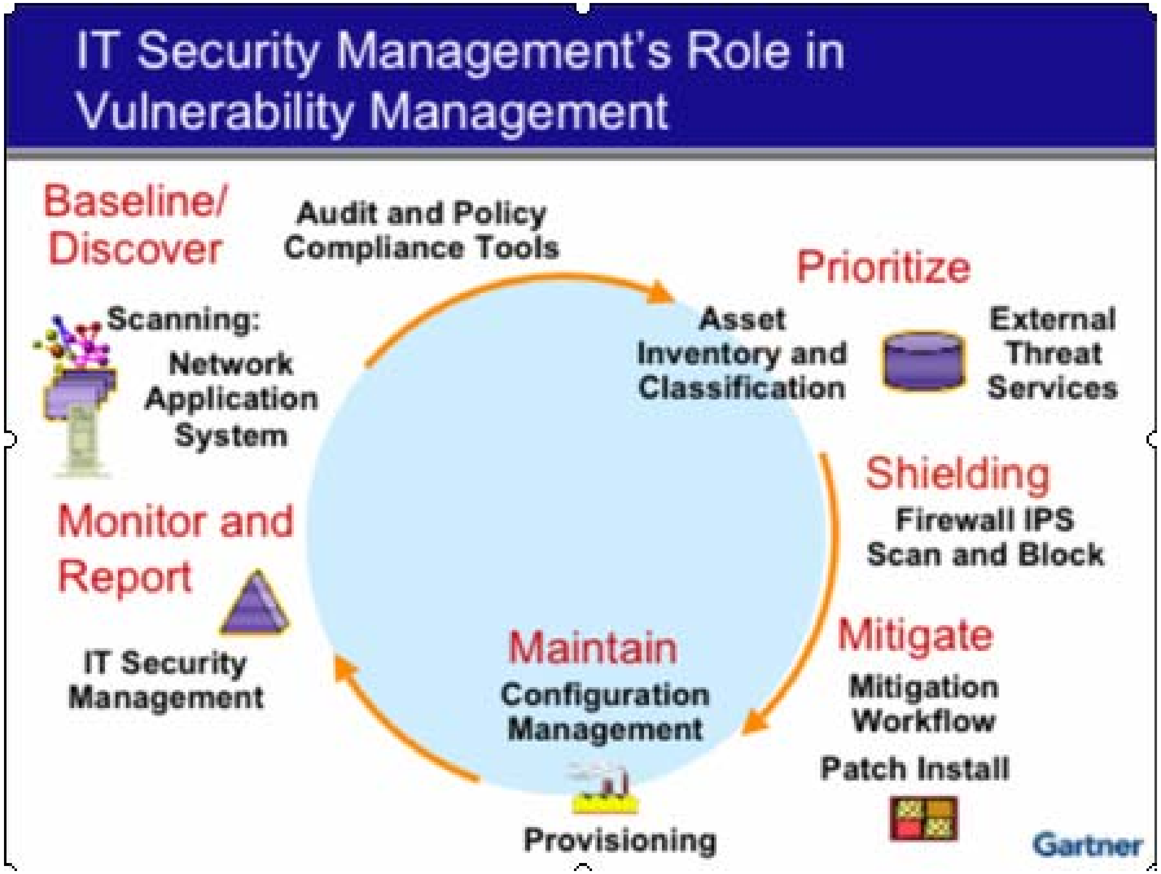
- Vulnerability Management Defined
- Vulnerability Management Goals
- Vulnerability Management Best Practices
- Enterprise Vulnerability Management Solution Requirements
- QualysGuard At a Glance
- Questions / Answers

Vulnerability Management Defined

- Vulnerability Management consists of the end-to-end processes from discovering your network, to assessing your assets, analyzing the results and remediating your exposures



Vulnerability Management Defined by Gartner



Vulnerability Management Goals

- Proactively identify vulnerabilities in hopes of remediating them before they are exploited manually (hacker) or automatically (worm / virus)
- Accurately understand the risk to the enterprise so mitigation can be prioritized
    - At any given point in time
    - Trending over time
- Augment, complement, & enhance other security solution investments (e.g. IDS, AV, FWs, etc.)

Vulnerability Management Best Practices

1. Know Your Network
2. Automate
   - Assess Consistently
   - Assess Regularly
3. Integrate
4. Distribute Use
   - Individuals
   - Scan Engines
5. Report on risk <u>and</u> vulnerabilities

Step 1: Know your Network

- Map your network, discover your hosts
  - Much of the network risk is introduced by unknown devices or devices that are not owned / company managed
    - Examples: pseudo-appliances, consultant’s & contractor’s laptops, non-standard or approved IP devices
- Deploy vulnerability scanners where necessary
  - Don’t limit your ability to assess risk to your enterprise by not having vulnerability scan engines where they are required
  - Must put dedicated scanners on the Internet, in each DMZ, and on the internal network

Step 2: Automate - Assess Consistently

- VM can be used to secure your enterprise proactively if you scan consistently
- Inconsistent scanning leads to false positives and false negatives
- Automation ⇨ Consistency
  - Scan for the same vulnerabilities (plus new vulnerabilities)
  - Scan the same ports / services
  - Scan at the same speed / network impact
  - Scan using the same scanner from the same network vantage point

Step 2: Automate - Assess Often

- Vulnerability Management can be a proactive security solution – if performed regularly
  - Must perform regular (e.g. weekly) assessments to react to accurate and current vulnerability data
  - Automate your network discovery and vulnerability scan tasks
- Imbed Vulnerability Management in existing and new processes
  - Device build processes
  - Monthly maintenance processes
  - Change management processes
- 80% of Qualys customers run recurring scans at least monthly
- 60% of Qualys customers run recurring scans weekly

Step 3: Integrate Your VM Solution

- Vulnerability data, when integrated with other security and operations tools and information, can be very powerful
  - Enhance your IDS investment; eliminate false positives by integrating VM data with IDS data
  - Integrate your VM solution with your change management / trouble ticketing solution or processes
  - Further automate patch application / patch management / configuration management
    - When missing patches or non-standard configurations are found on select devices, automate the remediation
  - Integrate to perform network quarantine

Step 4: Distribute Use - Individuals

- Enterprise Vulnerability Management tasks should be performed by more than just the security team
- Use ‘least privileges’ to assign select rights to:
  - Internal Audit
  - Systems and Network Administrators
  - Desktop Management teams
  - Technical and non-technical individuals

Step 4: Distribute Use – Scan Engines

- Vulnerabilities must be assessed from the independent 3rd party Internet perspective
  - ‘script kiddies’ are scanning you, shouldn’t you know what they can see?
- Vulnerabilities must be assessed from the DMZs
  - Need localized, authenticated scanning of these assets for full knowledge of vulnerabilities
- Vulnerabilities must be assessed from the Internal network
  - Majority of devices and least number of security layers reside here

Step 5: Report on Vulnerabilities AND Risk

- Vulnerability ≠ Risk
  - Vulnerabilities are exposures on assets due to software weakness or device misconfiguration
  - Risk considers the value of the asset and the mitigating factors in place against the vulnerability
- Example: same critical windows patch missing on 2 hosts; exploitable over port 80
  - Host 1: Corporate Web Server
  - Host 2: Joe User’s Laptop
  - The vulnerability on the 2 hosts are the same, but the risk to the organization is much higher on the corporate web server

Enterprise Vulnerability Management Solution Requirements

- Single solution for external and internal VM
  - Low TCO
  - Consolidated reporting
- Scaleable; easily deployable on distributed networks
- Network-based. Agents leave you exposed
  - With agents, it’s impossible to assess risk on all devices
    - Rogue devices, non-standard devices, network devices)
- Maintenance Free, Auto-updating
- Accurate & Comprehensive
- Secure
  - Data encryption
  - No impact on security architecture
- Clientless Web Interface

QualysGuard at a Glance

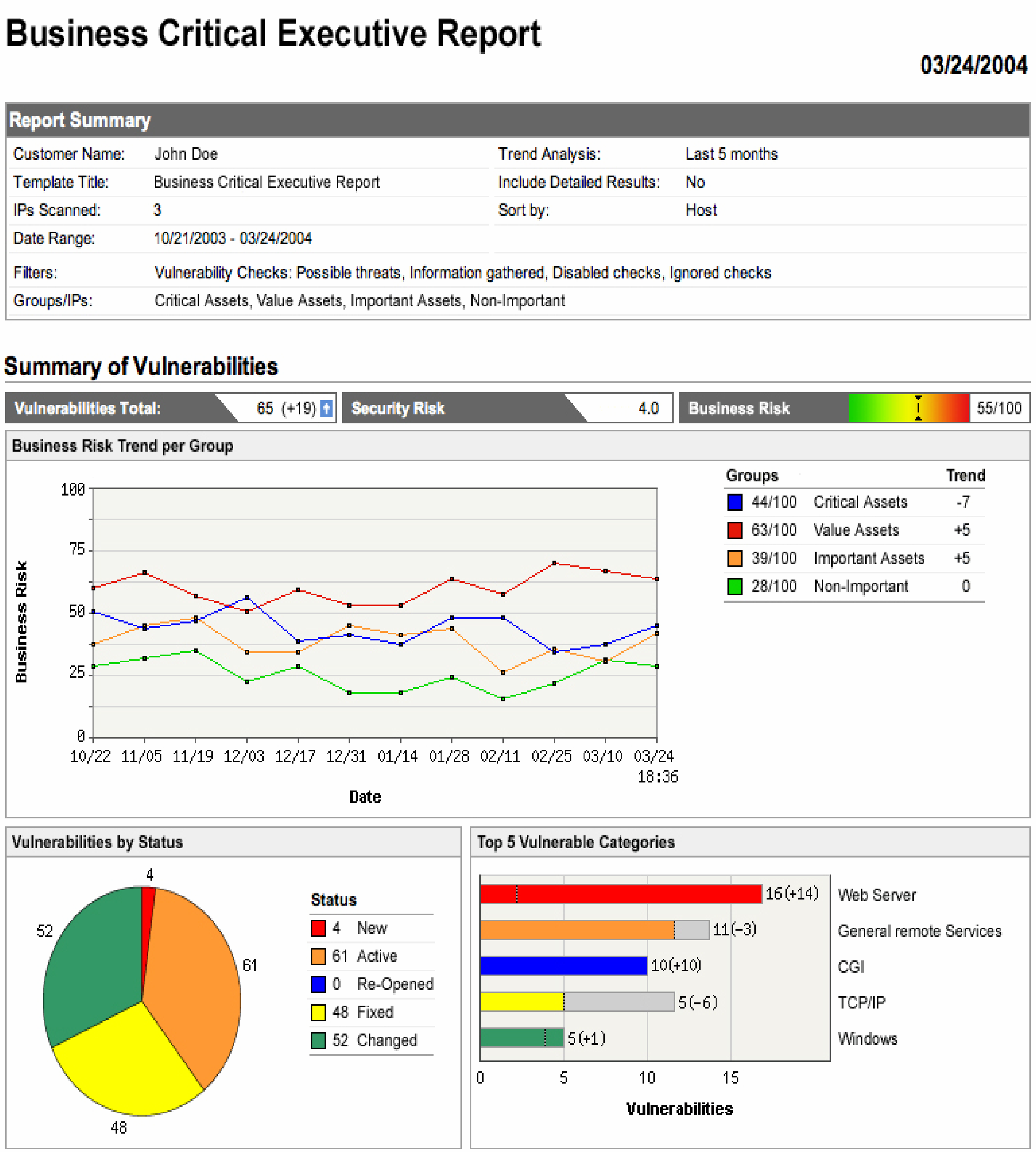
- Vulnerability Management solution available on demand
- Software-free, management free solution
  - Auto-updating
  - No software to install or maintain
- Industry’s most comprehensive Vulnerability KnowledgeBase ~ 3700 vulnerability signatures, updated daily
- Most accurate vulnerability scanner with less than .003% false positive rate
- Centralized repository automatically consolidates and aggregates all VM data for reporting

QualysGuard at a Glance

- Uniquely capable of vulnerability scanning from 3rd party Internet perspective, critical for assessing Internet risk
- Internal and localized DMZ vulnerability scanning using secure and hardened Scanner Appliances
- RBAC model allows organizations to easily distribute VM tasks
- Non-intrusive / non-disruptive scanning with auto-throttling intelligence
- Built-in comprehensive remediation workflow
- ‘Out of the Box’ XML API for seamless integration with other enterprise solutions

Sample QualysGuard Executive Report

- Summary charts show risk over time
- Can choose what data is represented
  - Over what period of time
  - Select assets to report on
  - etc.



Business Critical Executive Report

03/24/2004

Report Summary

Customer Name:	John Doe	Trend Analysis:	Last 5 months
Template Title:	Business Critical Executive Report	Include Detailed Results:	No
IPs Scanned:	3	Sort by:	Host
Date Range:	10/21/2003 - 03/24/2004		
Filters:	Vulnerability Checks: Possible threats, Information gathered, Disabled checks, Ignored checks		
Groups/IPs:	Critical Assets, Value Assets, Important Assets, Non-Important		

Summary of Vulnerabilities

Vulnerabilities Total: 65 (+19) | Security Risk 4.0 | Business Risk 55/100

Business Risk Trend per Group

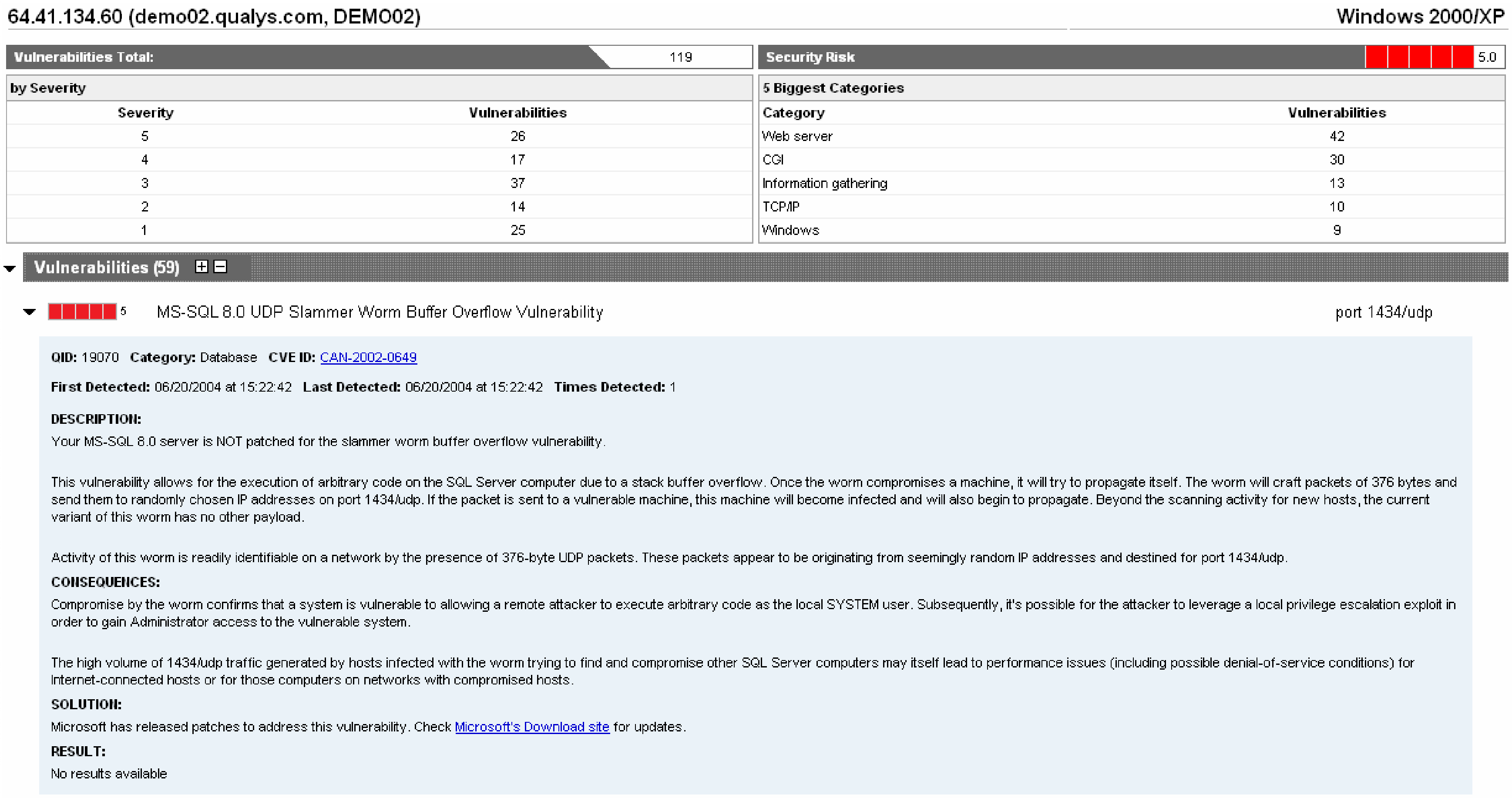
	Groups		Trend
🟦	44/100	Critical Assets	-7
🟥	63/100	Value Assets	+5
🟧	39/100	Important Assets	+5
🟩	28/100	Non-Important	0

Vulnerabilities by Status

	Status	
🟥	4	New
🟧	61	Active
🟦	0	Re-Opened
🟨	48	Fixed
🟩	52	Changed

Top 5 Vulnerable Categories

Sample Technical Vulnerability Report



64.41.134.60 (demo02.qualys.com, DEMO02) Windows 2000/XP

Vulnerabilities Total: 119

Security Risk 🟥🟥🟥🟥🟥 5.0

by Severity

Severity	Vulnerabilities
5	26
4	17
3	37
2	14
1	25

5 Biggest Categories

Category	Vulnerabilities
Web server	42
CGI	30
Information gathering	13
TCP/IP	10
Windows	9

Vulnerabilities (59) ⊞ ⊟

🟥🟥🟥🟥🟥 5 MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability port 1434/udp

QID: 19070 **Category:** Database **CVE ID:** CAN-2002-0649

First Detected: 06/20/2004 at 15:22:42 **Last Detected:** 06/20/2004 at 15:22:42 **Times Detected:** 1

DESCRIPTION:

Your MS-SQL 8.0 server is NOT patched for the slammer worm buffer overflow vulnerability.

This vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow. Once the worm compromises a machine, it will try to propagate itself. The worm will craft packets of 376 bytes and send them to randomly chosen IP addresses on port 1434/udp. If the packet is sent to a vulnerable machine, this machine will become infected and will also begin to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no other payload.

Activity of this worm is readily identifiable on a network by the presence of 376-byte UDP packets. These packets appear to be originating from seemingly random IP addresses and destined for port 1434/udp.

CONSEQUENCES:

Compromise by the worm confirms that a system is vulnerable to allowing a remote attacker to execute arbitrary code as the local SYSTEM user. Subsequently, it's possible for the attacker to leverage a local privilege escalation exploit in order to gain Administrator access to the vulnerable system.

The high volume of 1434/udp traffic generated by hosts infected with the worm trying to find and compromise other SQL Server computers may itself lead to performance issues (including possible denial-of-service conditions) for Internet-connected hosts or for those computers on networks with compromised hosts.

SOLUTION:

Microsoft has released patches to address this vulnerability. Check Microsoft's Download site for updates.

RESULT:

No results available

Where do you go from here?

- Trial QualysGuard for FREE

  http://www.qualys.com/worm

Q&A

Thank you

elevin@qualys.com