QUALYS

The Laws of Vulnerabilities

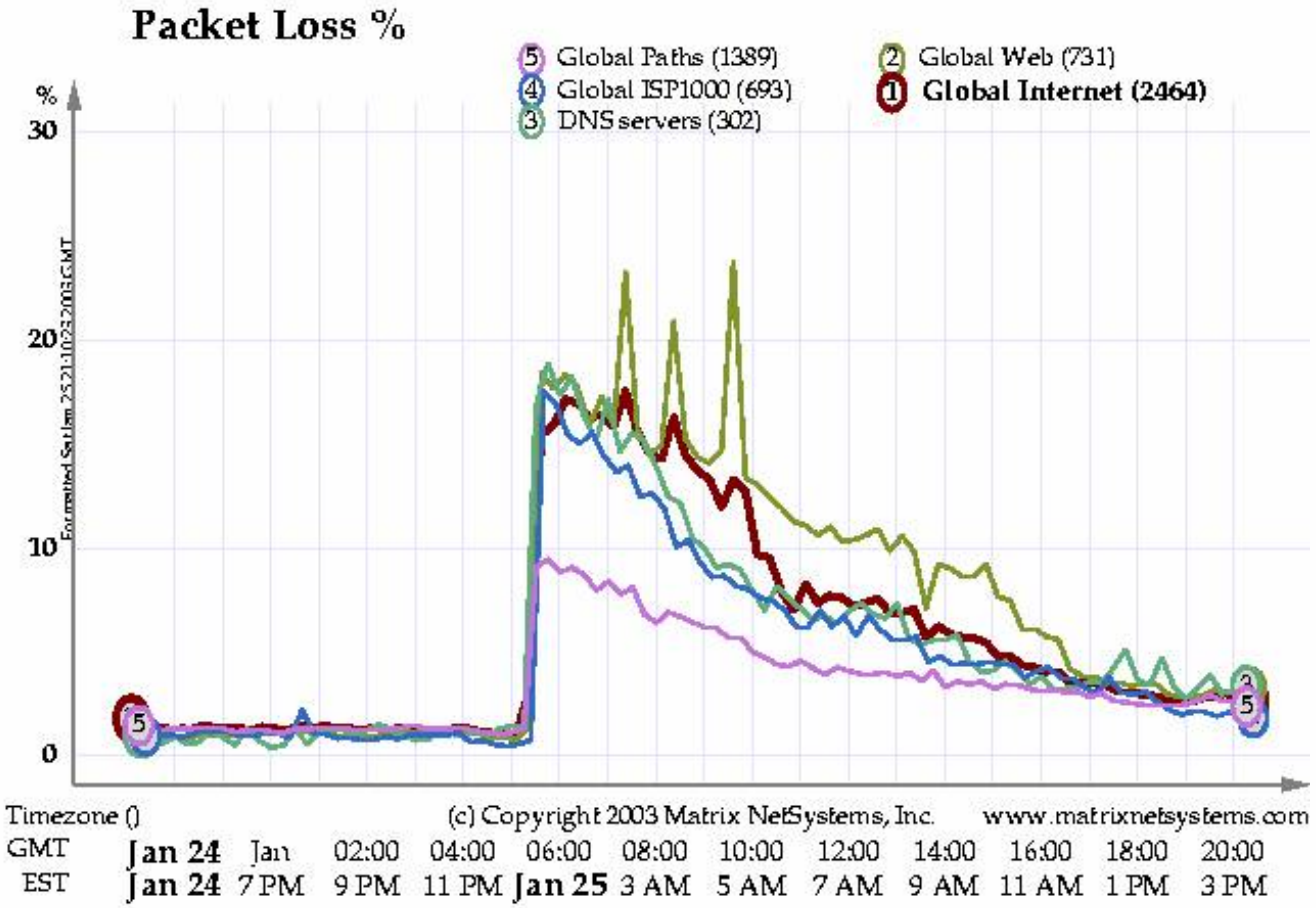
Gerhard Eschelbeck
CTO & VP Engineering, Qualys

February 5, 2004

SECURITY ON DEMAND

Windows Vulnerabilities in Action:

The Outbreak of the SQL Slammer Worm



SECURITY ON DEMAND

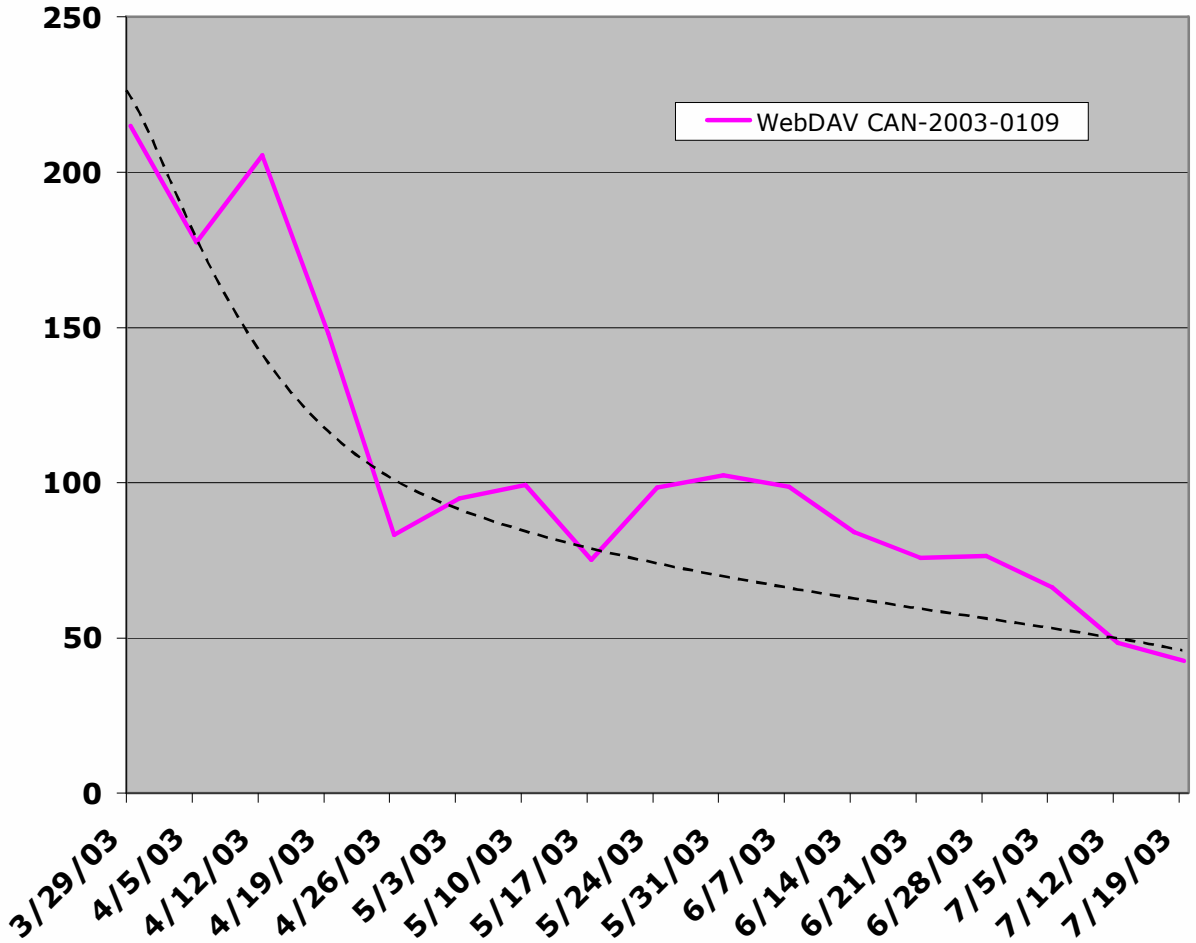
Security Threats are Evolving

- Leveraging known and unknown vulnerabilities
- Aggressive spreading via precompiled list of initial victims
- Active Payloads
- Leveraging polymorphic techniques and encryption to prevent discovery
- Multiple attack vectors
- Impact on new Technologies (Instant Messaging, Wireless Networks, Voice over IP,...)

Research

- **Understanding prevalence, window of exposure and lifespan of vulnerabilities in real world**
- **Timeframe: January 2002 - Ongoing**
- **Methodology: Automatic Data collection with statistical data only – no possible correlation to user or systems**
- **Largest collection of real-world vulnerability data:**
  - 3,011,000 IP-Scans
  - 1,905,000 total critical vulnerabilities
  - 2,054 unique vulnerabilities
  - 1,175 unique critical vulnerabilities

Microsoft WebDAV Vulnerability

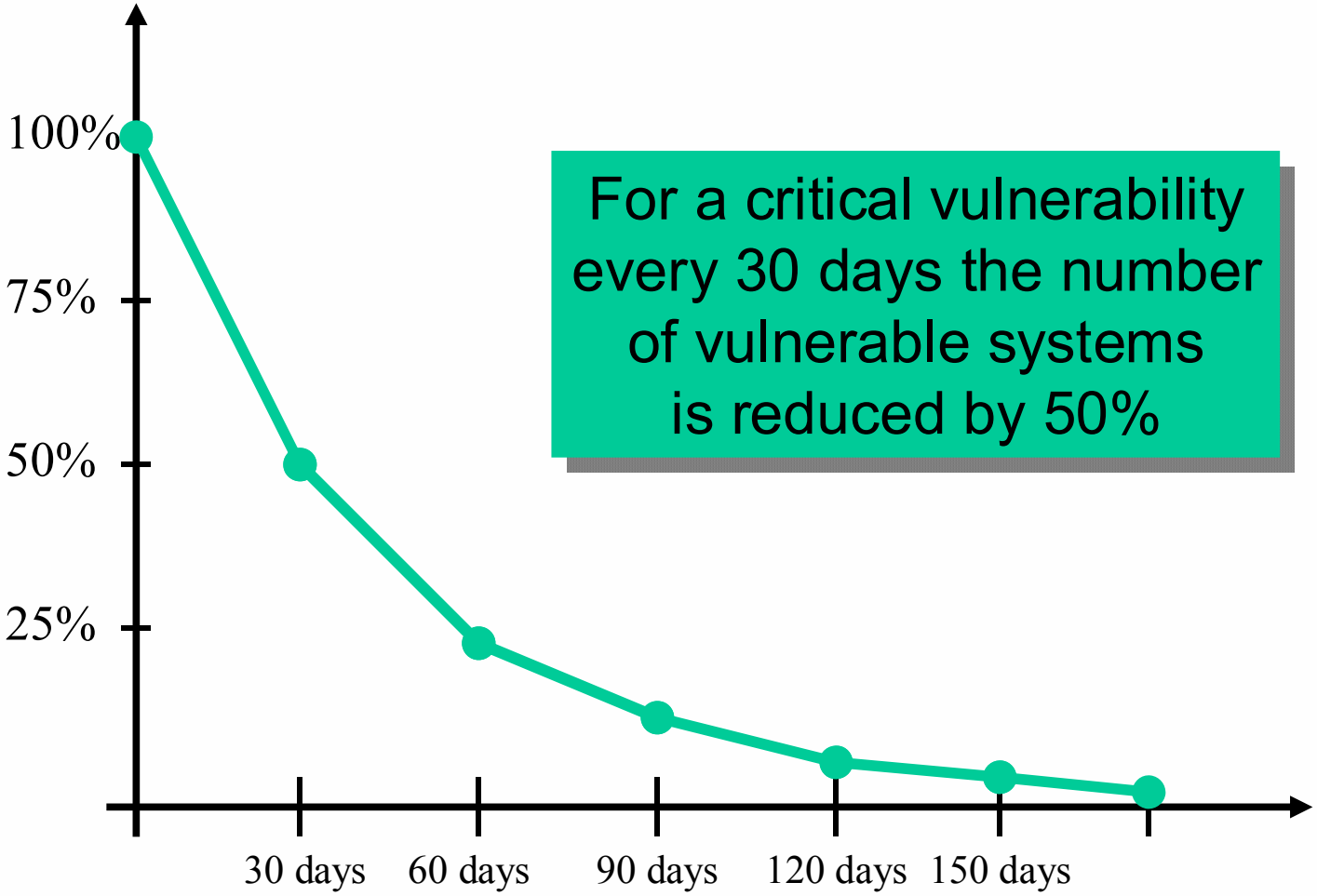


Microsoft Windows 2000
IIS WebDAV Buffer
Overflow Vulnerability

CAN-2003-0109
Qualys ID 86479

Released: March 2003

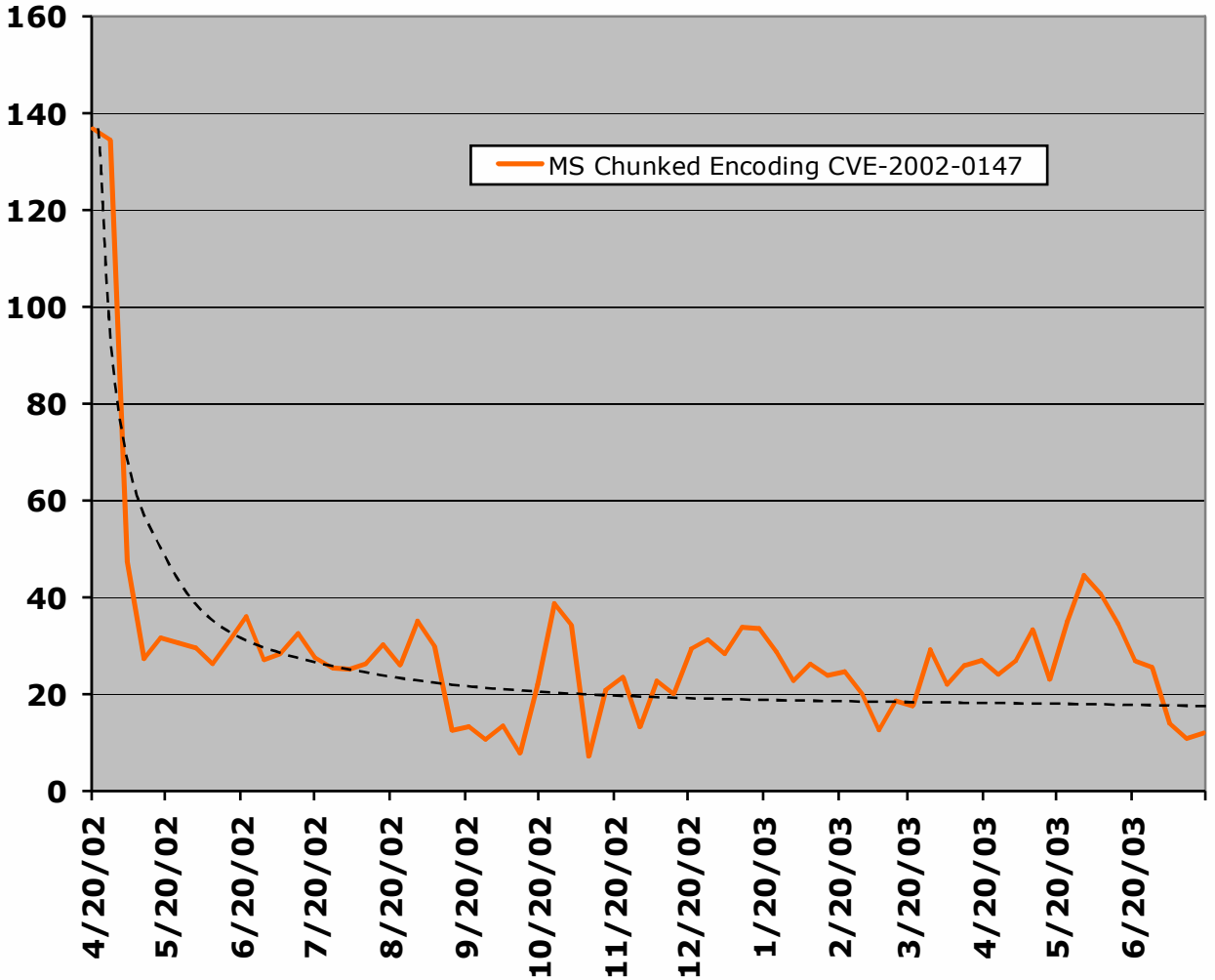
Vulnerability Half-Life



For a critical vulnerability every 30 days the number of vulnerable systems is reduced by 50%

SECURITY ON DEMAND

MS Chunked Encoding Overflow



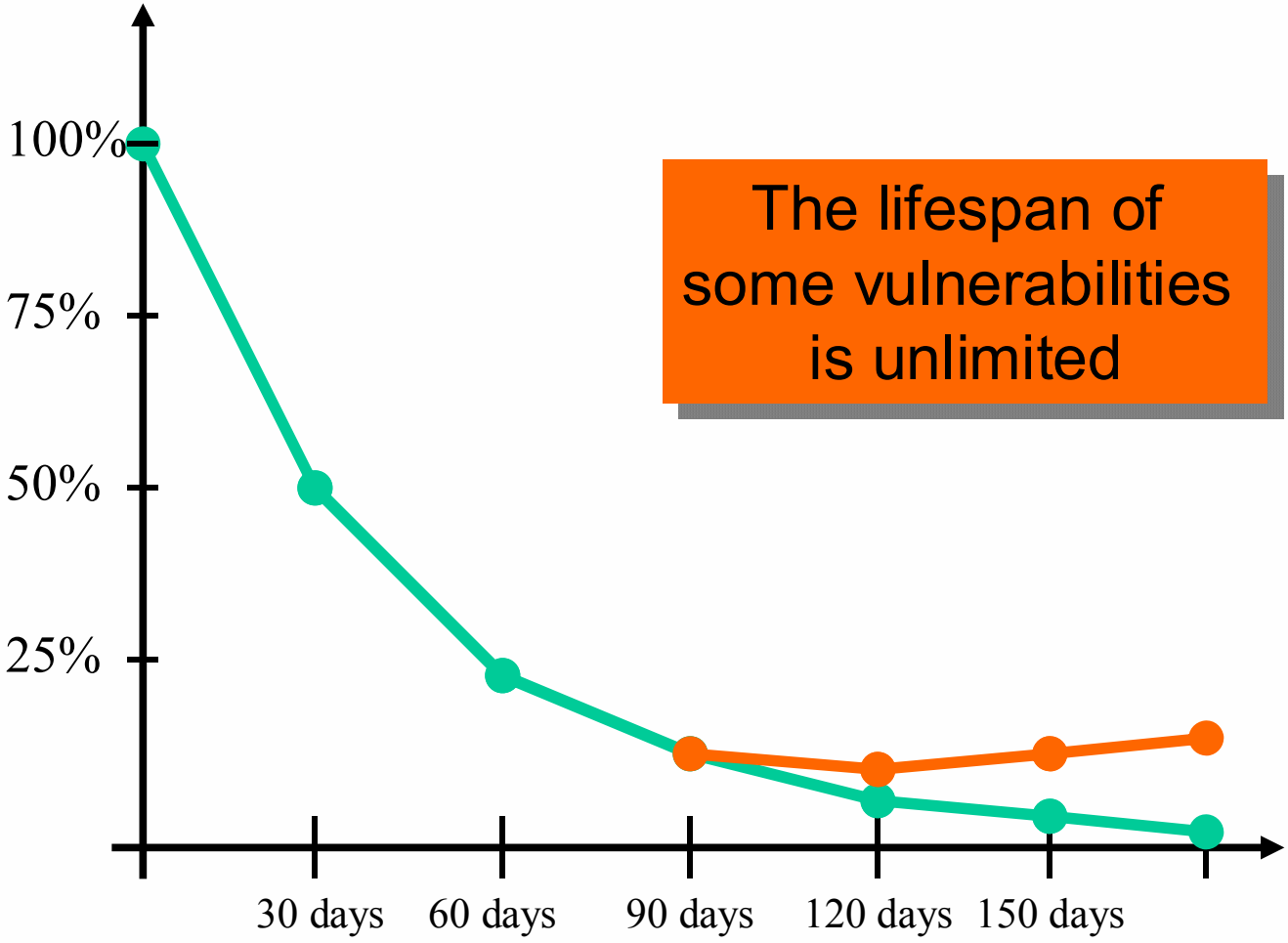
Microsoft IIS Chunked Encoding Heap Overflow Variant Vulnerability

CVE-2002-0147
Qualys ID 10571

Released: April 2002

SECURITY ON DEMAND

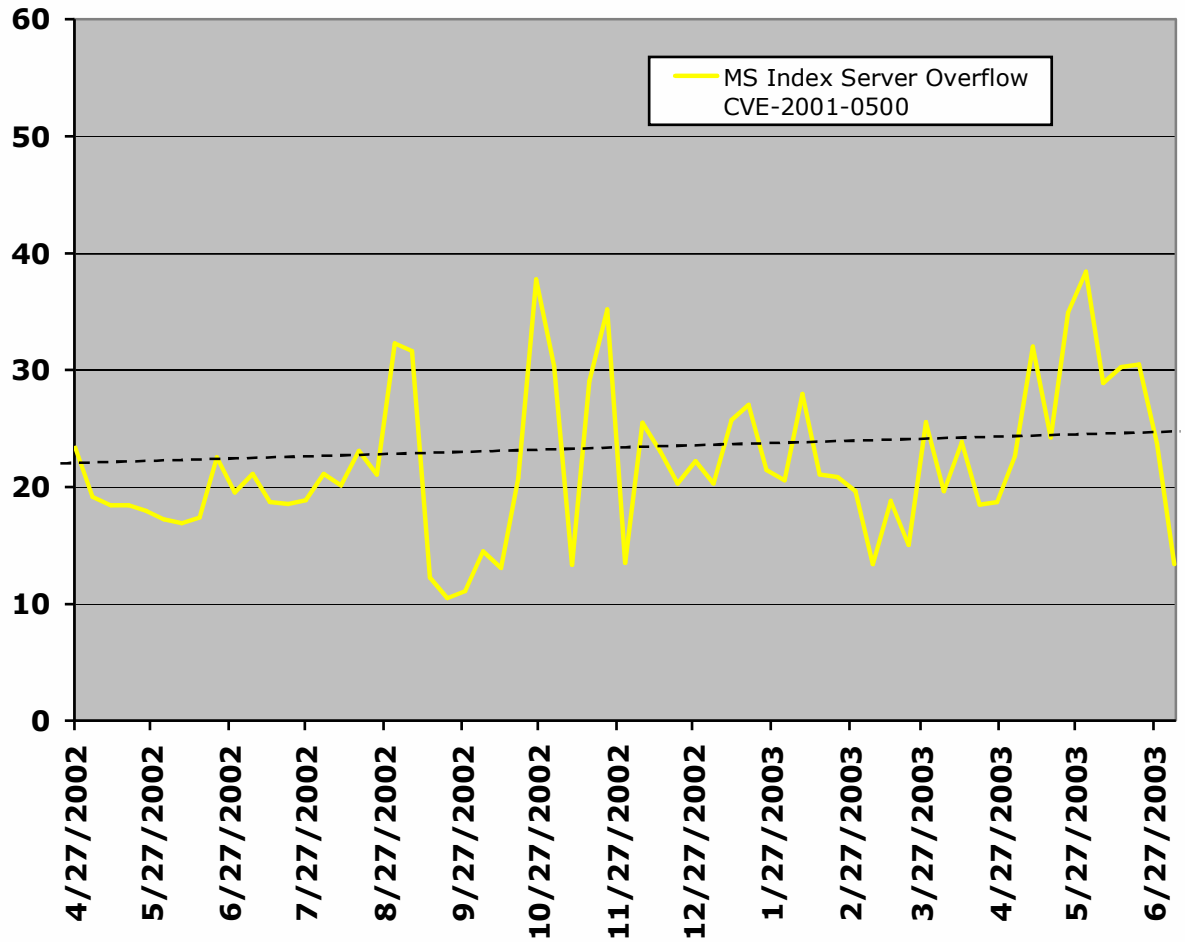
Vulnerability Lifespan



The lifespan of some vulnerabilities is unlimited

SECURITY ON DEMAND

MS Index Server Overflow (CodeRed)



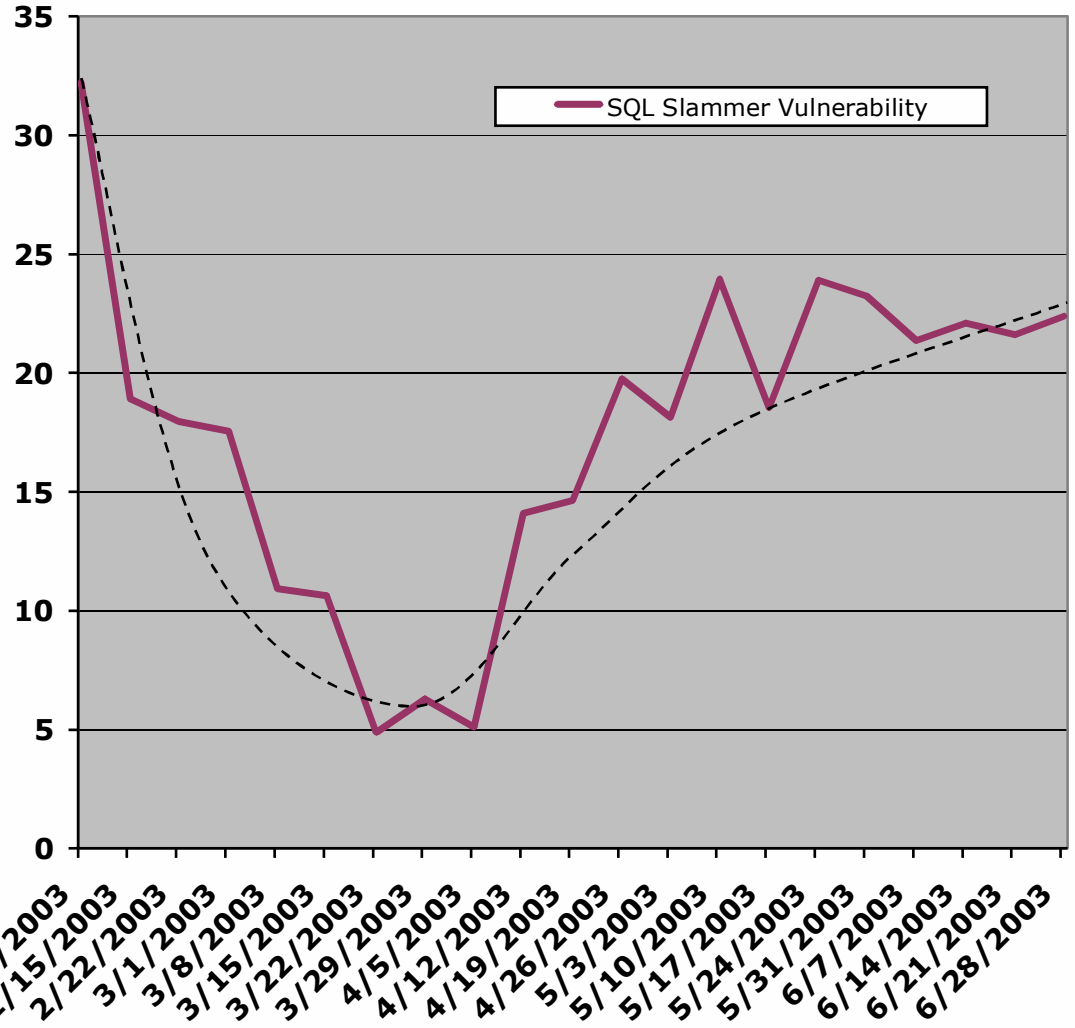
Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability

CVE-2001-0500
Qualys ID 86170

Released: June 2001

SECURITY ON DEMAND

SQL Slammer Vulnerability

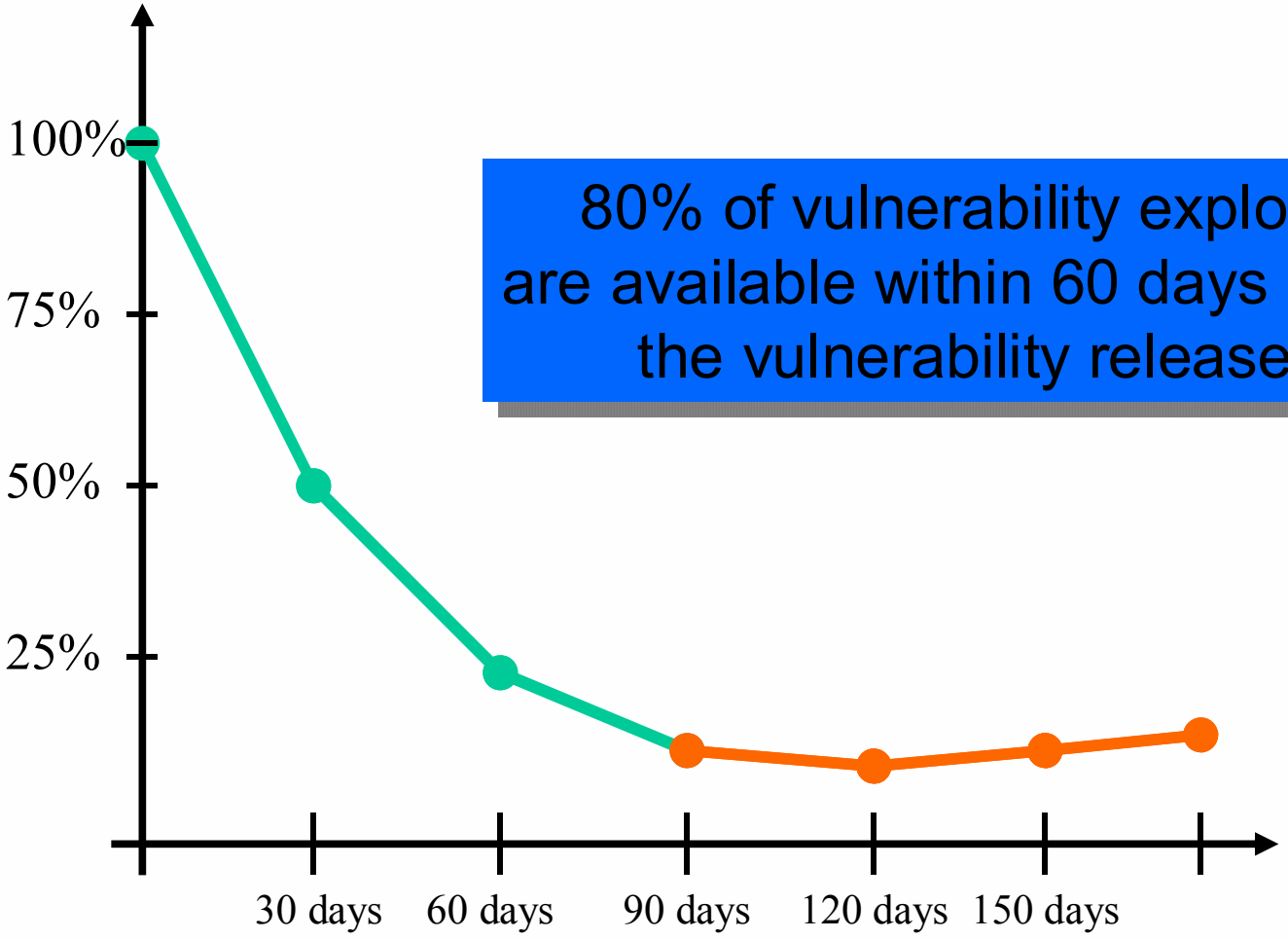


MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability

CAN-2002-0649
Qualys ID 19070

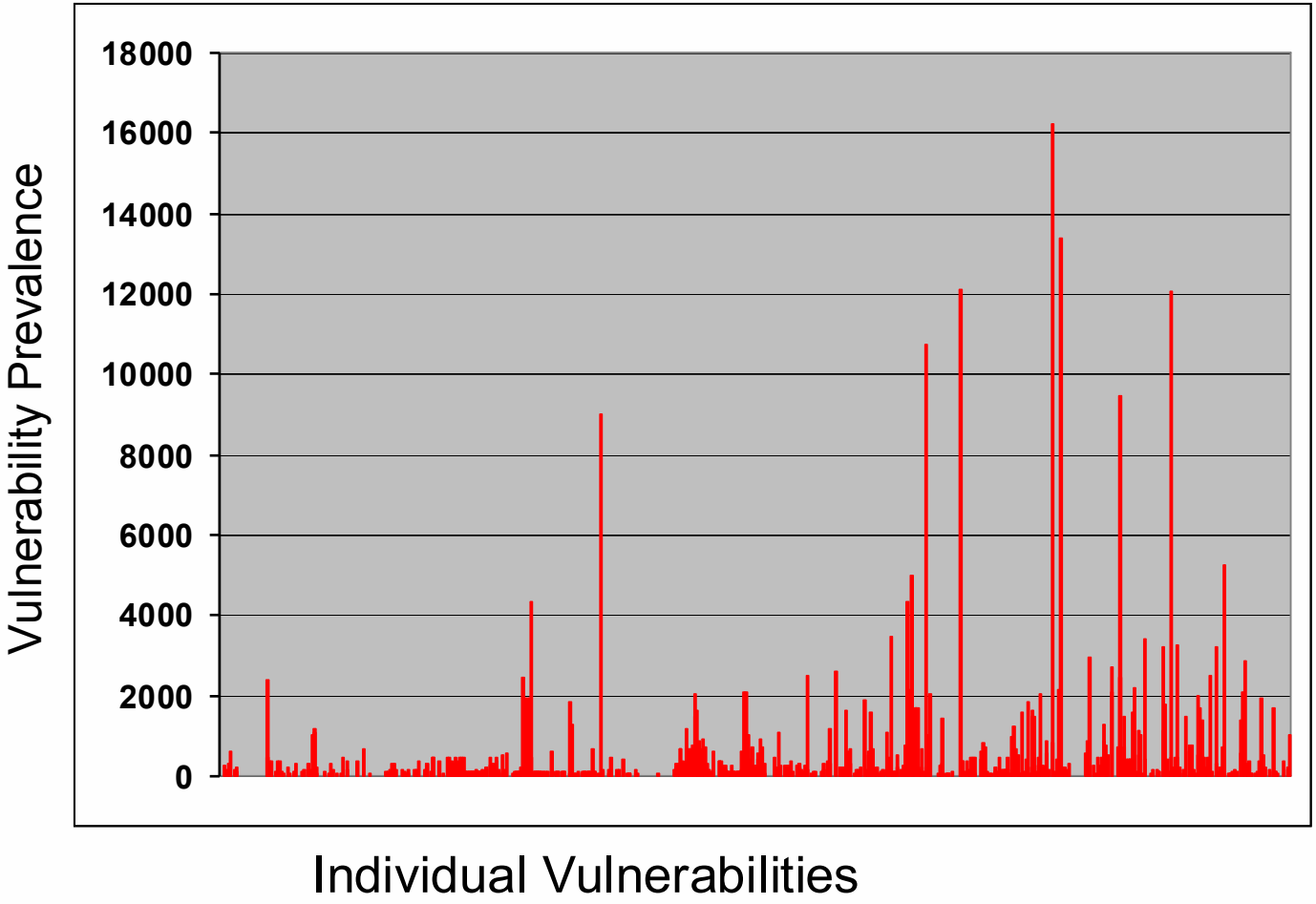
Released: July 2002

The Impact of an Exploit



80% of vulnerability exploits are available within 60 days after the vulnerability release

Mapping Vulnerability Prevalence



SECURITY ON DEMAND

The Changing Top of the Most Prevalent

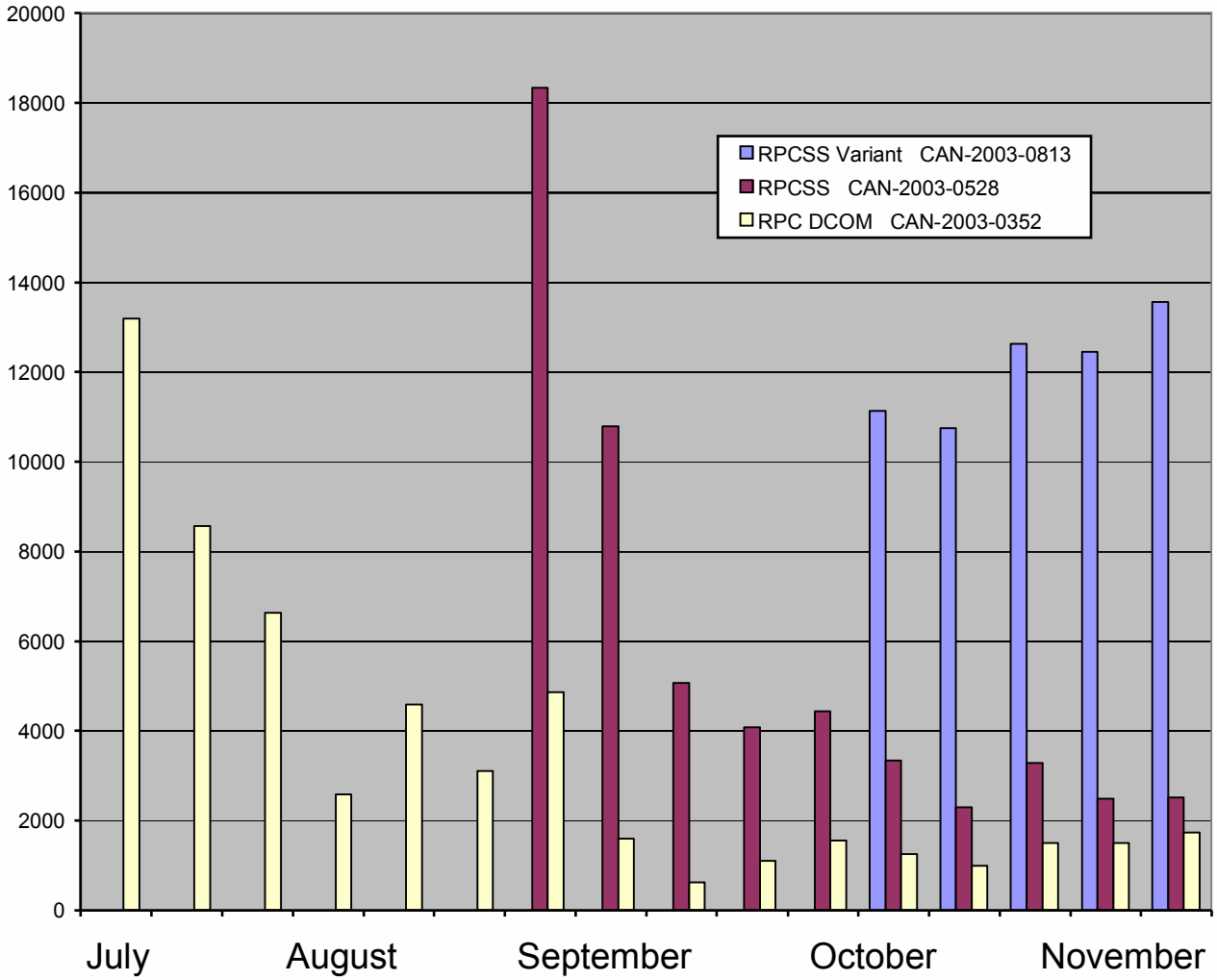
Vulnerability	CVE	Jul-02	Jan-03	Jul-03
Apache Mod_SSL Buffer Overflow Vulnerability	CVE-2002-0082	x		
Microsoft Exchange 2000 Malformed Mail Attribute DoS Vulnerability	CVE-2002-0368	x		
Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability	CVE-2001-0500	x	x	
Microsoft IIS			x	
Microsoft IIS			x	
Microsoft IIS			x	
Microsoft IIS			x	x
Microsoft IIS			x	x
Microsoft IIS			x	x
Microsoft IIS			x	x
Apache Chur			x	x
OpenSSH Ch			x	x
Multiple Vendor SNMP Request And Trap Handling Vulnerabilities			x	x
ISC BIND SIG Cached Resource Record Buffer Overflow (sigrec bug) Vulnerability	CAN-2002-1219		x	x
Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability	CAN-2003-0109			x
Sendmail Address Prescan Possible Memory Corruption Vulnerability	CAN-2003-0161			x
Microsoft SMB Request Handler Buffer Overflow Vulnerability	CAN-2003-0345			x
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CAN-2003-0352			x

50% of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities on an annual basis

10 Most Prevalent Vulnerabilities (as of February 5, 2004)

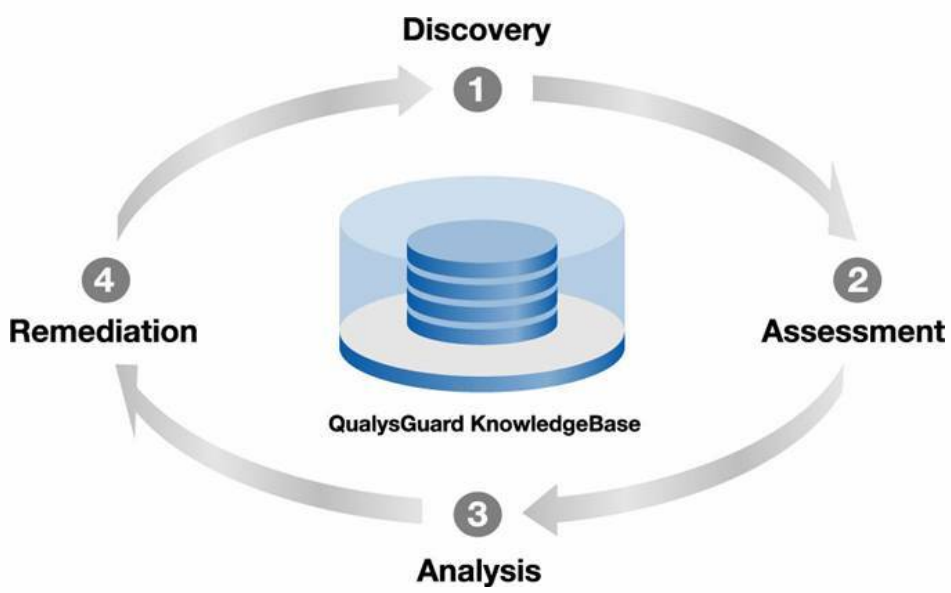
Microsoft IIS CGI Filename Decode Error Vulnerability	CVE-2001-0333
Microsoft IIS Malformed HTR Request Buffer Overflow Vulnerability	CVE-2002-0071
Apache Chunked-Encoding Memory Corruption Vulnerability	CVE-2002-0392
Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability	CAN-2003-0109
Sendmail Address Prescan Possible Memory Corruption Vulnerability	CAN-2003-0161
Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CAN-2003-0352
Microsoft Windows DCOM RPCSS Service Vulnerabilities	CAN-2003-0528
Microsoft Messenger Service Buffer Overrun Vulnerability	CAN-2003-0717
Microsoft Windows RPCSS Code Execution Variant Vulnerability	CAN-2003-0813
Writeable SNMP Information	No CVE assigned

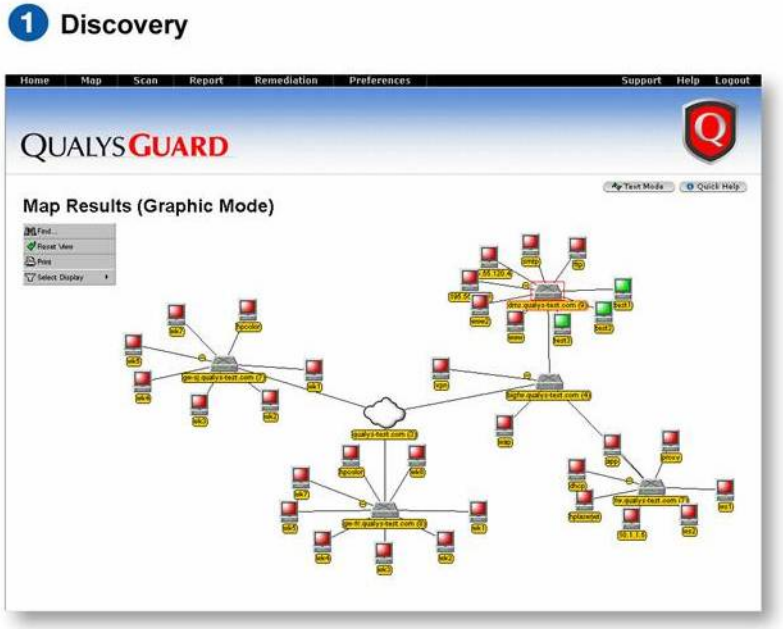
To Watch in 2004: Remote Procedure Call Vulnerabilities



SECURITY ON DEMAND

Proactive Approach to Vulnerability Management





SECURITY ON DEMAND

Qualys Mission

Automated Web Service for *ON-DEMAND* Network Security Audits and Vulnerability Management

- **Founded March, 1999**

Headquarters:	**Redwood Shores, California**
Global Offices:	**US, France, Germany, UK and Asia**
Advisors:	**Howard Schmidt, Becky Bace, Phil Zimmerman**
Employees:	**110+, 60+ in R&D and Operations**

- **Market Adoption**

  1,300 Customers – 200 Global 2,000

  100 new customers per month

SECURITY ON DEMAND

Thank You

ge@qualys.com

http://www.qualys.com

SECURITY ON DEMAND